DEC 23 1932

Journal für die reine und angewandte Mathematik

gegründet von A. L. Crelle 1826

Herausgegeben von

K. Hensel

H. Hasse L. Schlesinger

Wissenschaftlicher Beirat

H. Brandt / M. Dehn / G. Doetsch / A. Fraenkel / O. Haupt / F. Hausdorff
E. Hellinger / G. Kowalewski / H. Rademacher / K. Reidemeister
A. Rosenthal / C. Schaefer / W. Schmeidler / F. Schottky / O. Toeplitz

Band 168

Heft 4

Ausgegeben den 1. Dezember 1932

D 19

Walter de Gruyter & Co.

vormals G. J. Göschen'sche Verlagshandlung — J. Guttentag, Verlagsbuchhandlung — Georg Reimer — Karl J. Trübner — Veit & Comp.

Berlin W 10 und Leipzig

1932

Band 168. Heft 4.

Inhaltsverzeichnis.

	Seite
Taussky, Olga, Über eine Verschärfung des Hauptidealsatzes für algebraische Zahlkörper.	193
Koksma, J. F., und J. Popken, Zur Transzendenz von e^{π}	211
Wegener, U., Ein Satz über die Zerlegung von Primzahlen bestimmter arithmetischer Progressionen in algebraischen Zahlkörpern	231
Ore, Öystein, Formale Theorie der linearen Differentialgleichungen. (Zweiter Teil.) .	233

An unsere Mitarbeiter!

Es ist unbedingt notwendig, daß alle zur Einsendung gelangenden Manuskripte sowohl vollkommen druckfertig, als auch in gut lesbarer, möglichst Maschinen-Schrift gehalten sind, wobei die gotischen und griechischen wie überhaupt alle besonderen Typen durch Buntstift bezeichnet werden. Nachträgliche Korrekturen verursachen wesentliche Kosten, die sich naturgemäß auf die Preisgestaltung des Journals mit auswirken müssen. Machen sich also aus irgend einem Grunde Text-Änderungen eines Beitrages notwendig, so sind diese der Schriftleitung sofort mitzuteilen, wenn sie die endgültige Annahme und Weitergabe an den Verlag meldet; Korrekturen nach dem Vorliegen des Satzes dürfen sich ausschließlich auf die Verbesserung von Satzfehlern erstrecken.

Manuskripte, die den eingangs erwähnten Vorschriften entsprechen, ermöglichen auch der Schriftleitung eine raschere Prüfung als schwer leserliche und können infolgedessen schneller zum Druck gelangen.

Im Interesse des schnellen Erscheinens der einzelnen Hefte erhalten die Herren Verfasser grundsätzlich nur eine Korrektur ihrer Beiträge. Da seitens der Schriftleitung die Korrekturen in typographischer Hinsicht sorgfältige Lesung finden und die richtige Ausführung der Autor-Korrekturen genau überwacht wird, hoffen wir, auch so allen Wünschen gerecht zu werden.

Die Herren Verfasser erhalten von Abhandlungen bis zu 24 Seiten Umfang 100 Sonderabdrucke, von größeren Arbeiten 50 Sonderabdrucke kostenfrei, weitere gegen Berechnung.

Sendungen für das Journal erbittet die Redaktion ausschließlich unter der Adresse:

An die Redaktion des Journals für die reine und angewandte Mathematik

Professor Dr. Kurt Hensel, Marburg-Lahn, Behringweg 7.

Über eine Verschärfung des Hauptidealsatzes für algebraische Zahlkörper [1]).

Von *Olga Taussky* in Wien.

Herr Ph. Furtwängler hat die folgende Verschärfung des Hauptidealsatzes bewiesen: Ist für einen algebraischen Zahlkörper die absolute 2-Klassengruppe [2]) vom Typus $(2, 2, \ldots, 2)$, so läßt sich für sie eine Basis $c_1, c_2, \ldots, c_n$ so finden, daß jede Basisklasse c_i bereits in einem relativquadratischen unverzweigten Oberkörper in die Hauptklasse übergeht [3]).

Für beliebige Primzahlen l ist der entsprechende Satz nicht allgemein richtig. Wir werden aber hinreichende Bedingungen für den Grundkörper k formulieren, bei deren Bestehen der Hauptidealsatz in dieser verschärften Form gilt. Diese Bedingungen werden als Eigenschaften der zweistufigen [4]) Relativgruppe des zweiten Klassenkörpers in bezug auf den Grundkörper k auftreten. Weiter werden wir zeigen, daß sich mit Hilfe der zweistufigen Gruppe allein nicht entscheiden läßt, ob die Verschärfung allgemein gilt.

Es sei

$$\mathfrak{G} = S_1^{x_1} S_2^{x_2} \cdots S_n^{x_n} \mathfrak{C}, \qquad (0 \leqq x_i < l),$$

die zweistufige Relativgruppe des zweiten Klassenkörpers. Dabei bedeute $\mathfrak{C}$ die erste Ableitung von $\mathfrak{G}$, die $S_1, S_2, \ldots, S_n$ Repräsentanten der Basis für die Faktorgruppe $\mathfrak{G}/\mathfrak{C}$. Jedes S_j^l ist ein Element von $\mathfrak{C}$, läßt sich also als symbolisches Potenzprodukt der T_{ik} darstellen:

$$S_j^l = \prod_{i<k} T_{ik}^{g_{ik}^{(j)}(\Delta_1, \Delta_2, \ldots, \Delta_n)}, \qquad (j = 1, 2, \ldots, n).$$

Es gilt dann

Satz I. *Ist k ein algebraischer Zahlkörper, dessen absolute Klassengruppe [5]) außer der Hauptklasse nur Klassen der Ordnung l enthält, so lassen sich die Basisklassen $c_1, c_2, \ldots, c_n$ derart wählen, daß c_i bereits in einem unverzweigten relativ zyklischen Oberkörper vom Relativgrade l Hauptklasse wird, wenn die als Exponenten auftretenden ganzzahligen Polynome $g_{ik}^{(j)}(\Delta_1, \Delta_2, \ldots, \Delta_n)$ $(i, k, j = 1, 2, \ldots, n;\ i < k)$ mod. l nur Terme von einem Grad $\geqq l - 2$ enthalten.*

Da diese Bedingung für $l = 2$ immer erfüllt ist, enthält diese Aussage den Satz von Furtwängler.

---

[1]) Vgl. den Bericht über meinen Königsberger Vortrag, Jahresber. Deutsch. Math.-Vereinigung 40.

[2]) Unter der absoluten l-Klassengruppe versteht man die Faktorgruppe nach der Untergruppe, welche die absoluten Klassen mit zu l primer Ordnung bilden. Siehe Hasse, Bericht II, S. 174.

[3]) J. f. Math. **167**, S. 379.

[4]) Als zweistufig bezeichnen wir hier, sowie im folgenden die zweistufig metabelschen Gruppen. Siehe Hasse, Bericht II, S. 172.

[5]) Unter Klassengruppe werde im folgenden stets die l-Klassengruppe verstanden.

§ 1.

Betrachten wir die Struktur der in Betracht kommenden zweistufigen Gruppe von Primzahlpotenzordnung $\mathfrak{G}$ und ihrer Untergruppen. Es sei

$$\mathfrak{G} = S_1^{x_1} S_2^{x_2} \cdots S_n^{x_n} \mathfrak{C}, \qquad (0 \leqq x_i < l).$$

Dabei bedeute $\mathfrak{C}$ die erste Ableitung von $\mathfrak{G}$ und die S_i eine Basis für die Gruppe $\mathfrak{G}/\mathfrak{C}$. Jedes S_i^l ist ein Element von $\mathfrak{C}$, läßt sich daher durch die symbolischen Potenzen der $T_{ik} = S_i^{-1} S_k^{-1} S_i S_k$ darstellen [1]). Es gelten also die folgenden „Stammrelationen“:

$$S_j^l = \prod_{i<k} T_{ik}^{g_{ik}^{(j)}}, \qquad (j = 1, 2, \ldots, n),$$

wobei die $g_{ik}^{(j)}$ ganzzahlige Polynome in den $\Delta_r = S_r - 1$, $(r = 1, \ldots, n)$, sind. Die Gruppe $\mathfrak{G}$ ist vollständig gegeben, wenn wir die Stammrelationen und die sämtlichen Relationen zwischen den Kommutatoren T_{ik} kennen. Bekanntlich zerfallen die für die Existenz der Gruppe $\mathfrak{G}$ notwendigen und hinreichenden Relationen in zwei Typen:

I. Die Relationen, die sich aus den Stammrelationen ableiten lassen:

$$S_i^{l\Delta_k} = T_{ik}^{1+s_i+\cdots+s_i^{l-1}}, \qquad (i, k = 1, 2, \ldots, n).$$

II. Die Relationen, die unabhängig von den Stammrelationen zwischen den Kommutatoren jeder zweistufigen Gruppe bestehen:

$$T_{ik}^{\Delta_j} T_{kj}^{\Delta_i} T_{ji}^{\Delta_k} = E, \qquad \begin{pmatrix} i, k, j = 1, 2, \ldots, n \\ i \neq k \neq j \neq i \end{pmatrix}.$$

Die linken Seiten der Relationen II bezeichnen wir im folgenden stets mit T_{ikj}. Wir nennen s Relationen

$$T_j : \prod T_{ik}^{g_{ik}^{(j)}(\Delta_1, \Delta_2, \ldots, \Delta_n)} = E, \qquad (j = 1, 2, \ldots, s),$$

ein „vollständiges System“ von Relationen, wenn alle weiteren Relationen zwischen den T_{ik} als symbolische Potenzprodukte der T_j darstellbar sind.

Die Gruppen, auf welche es vor allem ankommen wird, haben folgende Eigenschaften:

1. Die in den Stammrelationen

$$S_j^l = \prod_{i<k} T_{ik}^{g_{ik}^{(j)}(\Delta_1, \Delta_2, \ldots, \Delta_n)}, \qquad (j = 1, 2, \ldots, n),$$

auftretenden Exponenten $g_{ik}^{(j)}$ enthalten mod. l nur Terme von einem Grad $\geqq l - 2$

2. Für jedes T_{ik} gilt, daß

$$T_{ik}^l = E$$

und, daß

$$T_{ik}^{\Delta_{j_1} \Delta_{j_2} \cdots \Delta_{j_{l-1}}} = E,$$

wenn $j_1, j_2, \ldots, j_{l-1}$ irgendwelche der Reihe $1, 2, \ldots, n$ entnommene Zahlen sind.

3. Die Relationen 2 bilden gemeinsam mit den Relationen II ein „vollständiges System“ von Relationen der Gruppe. (Wegen der Annahme 1 über die Stammrelationen sind nämlich die Relationen I ohne Bedeutung für die Gruppe).

Durch die Eigenschaften 1, 2, 3 ist die Gruppe $\mathfrak{G}$ gänzlich bestimmt, und zu jeder Wahl der Formen l—2-ten Grades $g_{ik}^{(j)}(\Delta_1, \Delta_2, \ldots, \Delta_n)$ (die Terme von einem Grade $\neq l - 2$ fallen nämlich wegen der Bedingungen 1, 2 weg) existiert eine zweistufige Gruppe, deren Elemente die geforderten Relationen und nur diese erfüllen [2]).

Betrachten wir nun die Untergruppen vom Index l von $\mathfrak{G}$. Wir erhalten sämtliche Normalteiler vom Index l von $\mathfrak{G}$, wenn wir die Exponenten in

---

[1]) Siehe Furtwängler, Hamb. Sem. Abh. 7, S. 18.

[2]) Siehe Schreier, Hamb. Sem. Abh. 4, S. 325.

$$S_1^{x_1} S_2^{x_2} \cdots S_n^{x_n} \mathfrak{C}, \qquad (0 \leqq x_i < l),$$

einer Bedingung

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n \equiv 0(l)$$

unterwerfen, wobei das System $a_1 \equiv a_2 \cdots \equiv a_n \equiv 0(l)$ ausgeschlossen ist, und zwei Kongruenzen, die sich nur um einen nicht durch l teilbaren Faktor unterscheiden, als identisch angesehen werden. Betrachten wir eine feste Basis $S_1, S_2, \ldots, S_n$, so besteht ein umkehrbar eindeutiges Entsprechen zwischen diesen linearen Kongruenzen und den Normalteilern vom Index l. Wir bezeichnen die durch

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n \equiv 0(l)$$

bestimmte Untergruppe von $\mathfrak{G}$ mit $\mathfrak{G}(a_1, a_2, \ldots, a_n)$ oder kurz $\mathfrak{G}(a)$. Den Unterkörper des zweiten Klassenkörpers, der zu $\mathfrak{G}(a)$ gehört, nennen wir $k(a_1, a_2, \ldots, a_n)$ oder $k(a)$. Der Klassenkörper über $k(a)$ gehört dann zur Kommutatorgruppe $\mathfrak{C}(a)$ der Gruppe $\mathfrak{G}(a)$. Sind

$$x_1^{(i)}, x_2^{(i)}, \ldots, x_n^{(i)}, \qquad (i = 1, 2, \ldots, n-1),$$

$n-1$ unabhängige Lösungen von

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n \equiv 0(l),$$

so ist

$$\mathfrak{G}(a) = \{S_1^{x_1^{(i)}} S_2^{x_2^{(i)}} \cdots S_n^{x_n^{(i)}}, \ (i = 1, 2, \ldots, n-1), \mathfrak{C}\}.$$

$\mathfrak{C}(a)$ wird symbolisch erzeugt aus den Kommutatoren von je zwei Elementen $S_1^{x_1^{(i)}} S_2^{x_2^{(i)}} \cdots S_n^{x_n^{(i)}}$ und den $(S_1^{x_1^{(i)}} S_2^{x_2^{(i)}} \cdots S_n^{x_n^{(i)}} - 1)$-ten Potenzen der Elemente von $\mathfrak{C}$. Beschränken wir uns gleich auf die Gruppen mit den Eigenschaften 1, 2, 3, so ist also

$$\mathfrak{C}(a) = \left\{ \begin{array}{ll} T_{ik}^{a_j} T_{kj}^{a_i} T_{ji}^{a_k}, & T_{ik}^{\Delta_1 x_1^{(j)} + \Delta_2 x_2^{(j)} + \cdots + \Delta_n x_n^{(j)}} \\ i \neq k \neq j \neq i & j = 1, 2, \ldots, n-1 \end{array} \right\}.$$

Über die Untergruppen $\mathfrak{G}(a)$ beweisen wir noch den folgenden

Hilfssatz 1. *Ist $\mathfrak{G}(a)$ die durch*

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n \equiv 0(l)$$

bestimmte Untergruppe, so sind von den $\binom{n}{3}$ Kommutatoren

$$T_{ik}^{a_j} T_{kj}^{a_i} T_{ji}^{a_k}, \qquad (i \neq k \neq j \neq i),$$

genau $\binom{n-1}{2}$ unabhängig.

Beweis. 1. Es sind höchstens $\binom{n-1}{2}$ der $T_{ik}^{a_j} T_{kj}^{a_i} T_{ji}^{a_k}$ unabhängig, da sie die Kommutatoren von $n-1$ Elementen sind.

2. Es sind mindestens $\binom{n-1}{2}$ unabhängige darunter. Wir führen den Beweis indirekt, indem wir zeigen, daß aus der Annahme, es bestünde zwischen je $\binom{n-1}{2}$ der $T_{ik}^{a_j} T_{kj}^{a_i} T_{ji}^{a_k}$ eine Relation, deren Exponenten nicht sämtlich durch l teilbar sind, folgen würde:

$$a_i \equiv 0(l), \qquad (i = 1, 2, \ldots, n).$$

Bezeichnen wir mit

$$(1) \qquad T_{1(\alpha)}, T_{2(\alpha)}, \ldots, T_{\binom{n-1}{2}(\alpha)}, \qquad (\alpha = 1, 2, \ldots, n),$$

die Reihe der $\binom{n-1}{2}$ Kommutatoren $T_{ik}^{a_j} T_{kj}^{a_i} T_{ji}^{a_k}$, in denen eine der Ziffern i, k, j mit der Ziffer α übereinstimmt. In jedem $T_{j(\alpha)}$ kommt der Index α in genau zweien der

§ 1.

Betrachten wir die Struktur der in Betracht kommenden zweistufigen Gruppe von Primzahlpotenzordnung $\mathfrak{G}$ und ihrer Untergruppen. Es sei

$$\mathfrak{G} = S_1^{x_1} S_2^{x_2} \cdots S_n^{x_n} \mathfrak{C}, \qquad (0 \leqq x_i < l).$$

Dabei bedeute $\mathfrak{C}$ die erste Ableitung von $\mathfrak{G}$ und die S_i eine Basis für die Gruppe $\mathfrak{G}/\mathfrak{C}$. Jedes S_i^l ist ein Element von $\mathfrak{C}$, läßt sich daher durch die symbolischen Potenzen der $T_{ik} = S_i^{-1} S_k^{-1} S_i S_k$ darstellen [1]). Es gelten also die folgenden „Stammrelationen“:

$$S_j^l = \prod_{i<k} T_{ik}^{g_{ik}^{(j)}}, \qquad (j = 1, 2, \ldots, n),$$

wobei die $g_{ik}^{(j)}$ ganzzahlige Polynome in den $\Delta_r = S_r - 1$, $(r = 1, \ldots, n)$, sind. Die Gruppe $\mathfrak{G}$ ist vollständig gegeben, wenn wir die Stammrelationen und die sämtlichen Relationen zwischen den Kommutatoren T_{ik} kennen. Bekanntlich zerfallen die für die Existenz der Gruppe $\mathfrak{G}$ notwendigen und hinreichenden Relationen in zwei Typen:

I. Die Relationen, die sich aus den Stammrelationen ableiten lassen:

$$S_i^{l\Delta_k} = T_{ik}^{1+s_i+\cdots+s_i^{l-1}}, \qquad (i, k = 1, 2, \ldots, n).$$

II. Die Relationen, die unabhängig von den Stammrelationen zwischen den Kommutatoren jeder zweistufigen Gruppe bestehen:

$$T_{ik}^{\Delta_j} T_{kj}^{\Delta_i} T_{ji}^{\Delta_k} = E, \qquad \begin{pmatrix} i, k, j = 1, 2, \ldots, n \\ i \neq k \neq j \neq i \end{pmatrix}.$$

Die linken Seiten der Relationen II bezeichnen wir im folgenden stets mit T_{ikj}. Wir nennen s Relationen

$$T_j : \prod T_{ik}^{r_{ik}^{(j)}(\Delta_1, \Delta_2, \ldots, \Delta_n)} = E, \qquad (j = 1, 2, \ldots, s),$$

ein „vollständiges System“ von Relationen, wenn alle weiteren Relationen zwischen den T_{ik} als symbolische Potenzprodukte der T_j darstellbar sind.

Die Gruppen, auf welche es vor allem ankommen wird, haben folgende Eigenschaften:

1. Die in den Stammrelationen

$$S_j^l = \prod_{i<k} T_{ik}^{g_{ik}^{(j)}(\Delta_1, \Delta_2, \ldots, \Delta_n)}, \qquad (j = 1, 2, \ldots, n),$$

auftretenden Exponenten $g_{ik}^{(j)}$ enthalten mod. l nur Terme von einem Grad $\geqq l - 2$

2. Für jedes T_{ik} gilt, daß

$$T_{ik}^l = E$$

und, daß

$$T_{ik}^{\Delta_{j_1} \Delta_{j_2} \cdots \Delta_{j_{l-1}}} = E,$$

wenn $j_1, j_2, \ldots, j_{l-1}$ irgendwelche der Reihe $1, 2, \ldots, n$ entnommene Zahlen sind.

3. Die Relationen 2 bilden gemeinsam mit den Relationen II ein „vollständiges System“ von Relationen der Gruppe. (Wegen der Annahme 1 über die Stammrelationen sind nämlich die Relationen I ohne Bedeutung für die Gruppe).

Durch die Eigenschaften 1, 2, 3 ist die Gruppe $\mathfrak{G}$ gänzlich bestimmt, und zu jeder Wahl der Formen l—2-ten Grades $g_{ik}^{(j)}(\Delta_1, \Delta_2, \ldots, \Delta_n)$ (die Terme von einem Grade $\neq l - 2$ fallen nämlich wegen der Bedingungen 1, 2 weg) existiert eine zweistufige Gruppe, deren Elemente die geforderten Relationen und nur diese erfüllen [2]).

Betrachten wir nun die Untergruppen vom Index l von $\mathfrak{G}$. Wir erhalten sämtliche Normalteiler vom Index l von $\mathfrak{G}$, wenn wir die Exponenten in

---

[1]) Siehe Furtwängler, Hamb. Sem. Abh. 7, S. 18.

[2]) Siehe Schreier, Hamb. Sem. Abh. 4, S. 325.

$$S_1^{x_1} S_2^{x_2} \cdots S_n^{x_n} \mathfrak{C}, \qquad (0 \leqq x_i < l),$$

einer Bedingung

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n \equiv 0(l)$$

unterwerfen, wobei das System $a_1 \equiv a_2 \cdots \equiv a_n \equiv 0(l)$ ausgeschlossen ist, und zwei Kongruenzen, die sich nur um einen nicht durch l teilbaren Faktor unterscheiden, als identisch angesehen werden. Betrachten wir eine feste Basis $S_1, S_2, \ldots, S_n$, so besteht ein umkehrbar eindeutiges Entsprechen zwischen diesen linearen Kongruenzen und den Normalteilern vom Index l. Wir bezeichnen die durch

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n \equiv 0(l)$$

bestimmte Untergruppe von $\mathfrak{G}$ mit $\mathfrak{G}(a_1, a_2, \ldots, a_n)$ oder kurz $\mathfrak{G}(a)$. Den Unterkörper des zweiten Klassenkörpers, der zu $\mathfrak{G}(a)$ gehört, nennen wir $k(a_1, a_2, \ldots, a_n)$ oder $k(a)$. Der Klassenkörper über $k(a)$ gehört dann zur Kommutatorgruppe $\mathfrak{C}(a)$ der Gruppe $\mathfrak{G}(a)$. Sind

$$x_1^{(i)}, x_2^{(i)}, \ldots, x_n^{(i)}, \qquad (i = 1, 2, \ldots, n-1),$$

$n-1$ unabhängige Lösungen von

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n \equiv 0(l),$$

so ist

$$\mathfrak{G}(a) = \{S_1^{x_1^{(i)}} S_2^{x_2^{(i)}} \cdots S_n^{x_n^{(i)}}, \ (i = 1, 2, \ldots, n-1), \mathfrak{C}\}.$$

$\mathfrak{C}(a)$ wird symbolisch erzeugt aus den Kommutatoren von je zwei Elementen $S_1^{x_1^{(i)}} S_2^{x_2^{(i)}} \cdots S_n^{x_n^{(i)}}$ und den $(S_1^{x_1^{(i)}} S_2^{x_2^{(i)}} \cdots S_n^{x_n^{(i)}} - 1)$-ten Potenzen der Elemente von $\mathfrak{C}$. Beschränken wir uns gleich auf die Gruppen mit den Eigenschaften 1, 2, 3, so ist also

$$\mathfrak{C}(a) = \left\{ \begin{array}{ll} T_{ik}^{a_j} T_{kj}^{a_i} T_{ji}^{a_k}, & T_{ik}^{\Delta_1 x_1^{(j)} + \Delta_2 x_2^{(j)} + \cdots + \Delta_n x_n^{(j)}} \\ i \neq k \neq j \neq i & j = 1, 2, \ldots, n-1 \end{array} \right\}.$$

Über die Untergruppen $\mathfrak{G}(a)$ beweisen wir noch den folgenden

Hilfssatz 1. *Ist $\mathfrak{G}(a)$ die durch*

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n \equiv 0(l)$$

bestimmte Untergruppe, so sind von den $\binom{n}{3}$ Kommutatoren

$$T_{ik}^{a_j} T_{kj}^{a_i} T_{ji}^{a_k}, \qquad (i \neq k \neq j \neq i),$$

genau $\binom{n-1}{2}$ unabhängig.

Beweis. 1. Es sind höchstens $\binom{n-1}{2}$ der $T_{ik}^{a_j} T_{kj}^{a_i} T_{ji}^{a_k}$ unabhängig, da sie die Kommutatoren von $n-1$ Elementen sind.

2. Es sind mindestens $\binom{n-1}{2}$ unabhängige darunter. Wir führen den Beweis indirekt, indem wir zeigen, daß aus der Annahme, es bestünde zwischen je $\binom{n-1}{2}$ der $T_{ik}^{a_j} T_{kj}^{a_i} T_{ji}^{a_k}$ eine Relation, deren Exponenten nicht sämtlich durch l teilbar sind, folgen würde:

$$a_i \equiv 0(l), \qquad (i = 1, 2, \ldots, n).$$

Bezeichnen wir mit

$$(1) \qquad T_{1(\alpha)}, T_{2(\alpha)}, \ldots, T_{\binom{n-1}{2}(\alpha)}, \qquad (\alpha = 1, 2, \ldots, n),$$

die Reihe der $\binom{n-1}{2}$ Kommutatoren $T_{ik}^{a_j} T_{kj}^{a_i} T_{ji}^{a_k}$, in denen eine der Ziffern i, k, j mit der Ziffer α übereinstimmt. In jedem $T_{j(\alpha)}$ kommt der Index α in genau zweien der

T_{ik} vor. Jedes $T_{\alpha i}$ tritt daher in der Reihe (1) genau $n-2$ mal, jedes T_{ik}, $i, k \neq \alpha$, genau einmal, und zwar mit dem Exponenten a_α auf. Wäre die Behauptung 2 nicht richtig, so müßte zwischen den Elementen jeder Reihe (1) eine Relation

$$T_{1(\alpha)}^{r_{1(\alpha)}} T_{2(\alpha)}^{r_{2(\alpha)}} \cdots T_{\binom{n-1}{2}(\alpha)}^{r_{\binom{n-1}{2}(\alpha)}} = E \tag{2}$$

bestehen, wobei für jeden Wert α mindestens eine der Zahlen $r_{i(\alpha)} \not\equiv 0(l)$ ist. Wegen der Voraussetzungen 2 und 3 über die Gruppe $\mathfrak{G}$ folgt aus jeder Beziehung (2)

$$a_\alpha r_{i(\alpha)} \equiv 0(l), \quad i = 1, 2, \ldots, \binom{n-1}{2},$$

also

$$a_\alpha \equiv 0(l).$$

Wir gelangen so, wenn wir $\alpha = 1, 2, \ldots, n$ setzen, zu dem Widerspruch

$$a_1 \equiv a_2 \equiv \cdots \equiv a_n \equiv 0(l).$$

§ 2.

Wir werden die Richtigkeit von Satz I erschließen, indem wir ihn zunächst nur für die in § 1 behandelten speziellen zweistufigen Gruppen beweisen:

Satz II. *Es sei k ein algebraischer Zahlkörper, dessen Idealklassen mit Ausnahme der Hauptklasse die Ordnung l haben. Die zweistufige Relativgruppe des 2. Klassenkörpers in bezug auf k besitze die folgenden, ein „vollständiges System" bildenden Relationen: $T_{ik}^{l} = E$, $T_{ik}^{\Delta_{j_1} \Delta_{j_2} \cdots \Delta_{j_{l-1}}} = E$, $T_{ik}^{\Delta_j} T_{kj}^{\Delta_i} T_{ji}^{\Delta_k} = E$. Die Stammrelationen seien $S_j^l = \Pi T_{ik}^{g_{ik}^{(j)}}$ und dabei die $g_{ik}^{(j)}$ Formen in den $\Delta_1, \Delta_2, \ldots, \Delta_n$ vom Grade $l-2$. Man kann dann eine Basis $c_1, c_2, \ldots, c_n$ für die Klassengruppe von k so wählen, daß die Basisklassen in n relativ zyklischen unverzweigten Oberkörpern $k_1, k_2, \ldots, k_n$ in die Hauptklasse übergehen, und daß in jedem Körper k_i nur eine Klasse von k Hauptklasse wird.*

Aus Satz II folgt die Richtigkeit von Satz I. Denn wenn eine Klasse von k in einem unverzweigten relativ zyklischen Oberkörper $k(a)$ vom Relativgrad l in die Hauptklasse übergeht, so bedeutet dies, daß die der Klasse im Oberkörper entsprechende Substitution das Einheitselement der Relativgruppe des zugehörigen Klassenkörpers ist. Fassen wir diesen Klassenkörper als Unterkörper des zweiten Klassenkörpers über k auf, so ist das Einheitselement seiner Relativgruppe in bezug auf $k(a)$ die Gruppe $\mathfrak{C}(a)$. Haben wir von einer Klasse nachgewiesen, daß sie bei Zugrundelegung einer bestimmten zweistufigen Gruppe in $k(a)$ in die Hauptklasse übergeht, dann muß sie in demselben Oberkörper auch dann Hauptklasse werden, wenn die Klassengruppe des Klassenkörpers über k weniger umfassend angenommen wird. Den umgekehrten Schluß kann man hingegen dann und nur dann machen, wenn in $k(a)$ nur *eine* Klasse Hauptklasse wird.

Dem Beweise seien einige Hilfssätze vorausgeschickt.

Hilfssatz 2. *Sind $x_1^{(i)}, x_2^{(i)}, \ldots, x_n^{(i)}$, $(i = 1, 2, \ldots, n-1)$, $n-1$ unabhängige Lösungen der Kongruenz*

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n \equiv 0(l),$$

so ist eine beliebige Form $g(\Delta_1, \Delta_2, \ldots, \Delta_n)$ in den $\Delta_1, \Delta_2, \ldots, \Delta_n$ einem Ausdruck

$$\sum_{i=1}^{n-1} (\Delta_1 x_1^{(i)} + \Delta_2 x_2^{(i)} + \cdots + \Delta_n x_n^{(i)}) h_i(\Delta_1, \Delta_2, \ldots, \Delta_n),$$

wobei die h_i wieder Formen in den $\Delta_1, \Delta_2, \ldots, \Delta_n$ bedeuten, dann und nur dann mod. l kongruent, wenn

$$g(a_1, a_2, \ldots, a_n) \equiv 0(l).$$

Beweis. 1. Die Bedingung ist notwendig. Denn ist $g(\Delta_1, \Delta_2, \ldots, \Delta_n)$ in der obigen Weise darstellbar, und setzen wir

$$\Delta_i = a_i, \qquad (i = 1, 2, \ldots, n),$$

so ist, da

$$a_1 x_1^{(i)} + a_2 x_2^{(i)} + \cdots + a_n x_n^{(i)} \equiv 0(l),$$

auch

$$g(a_1, a_2, \ldots, a_n) \equiv 0(l).$$

2. Die Bedingung ist hinreichend.
Es sei also $g(a_1, a_2, \ldots, a_n) \equiv 0(l)$. Wir setzen

$$\Delta_1 x_1^{(i)} + \Delta_2 x_2^{(i)} + \cdots + \Delta_n x_n^{(i)} = \bar{\Delta}_i, \qquad (i = 1, 2, \ldots, n-1),$$

und bestimmen

$$\Delta_1 x_1^{(n)} + \Delta_2 x_2^{(n)} + \cdots + \Delta_n x_n^{(n)} = \bar{\Delta}_n,$$

so daß

$$|x_i^{(j)}| \equiv 1(l).$$

Wir setzen ferner

$$a_1 x_1^{(j)} + a_2 x_2^{(j)} + \cdots + a_n x_n^{(j)} = \bar{a}_j, \qquad (j = 1, 2, \ldots, n).$$

$g(\Delta_1, \Delta_2, \ldots, \Delta_n)$ geht bei dieser Substitution über in eine Form $\bar{g}(\bar{\Delta}_1, \bar{\Delta}_2, \ldots, \bar{\Delta}_n)$. Da $g(a_1, a_2, \ldots, a_n) \equiv 0(l)$ ist, gilt auch

$$\bar{g}(\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_n) \equiv \bar{g}(0, 0, \ldots, 0, \bar{a}_n) \equiv 0(l).$$

Dann ist aber auch

$$\bar{g}(0, 0, \ldots, 0, \bar{\Delta}_n) \equiv 0(l),$$

d. h. $\bar{g}(\bar{\Delta}_1, \bar{\Delta}_2, \ldots, \bar{\Delta}_n)$ enthält mod. l nur Glieder, die wenigstens einen der Faktoren $\bar{\Delta}_1, \bar{\Delta}_2, \ldots, \bar{\Delta}_n$ enthalten, also

$$\bar{g}(\bar{\Delta}_1, \bar{\Delta}_2, \ldots, \bar{\Delta}_n) \equiv \sum_{i=1}^{n-1} \bar{\Delta}_i \bar{h}_i(\bar{\Delta}_1, \bar{\Delta}_2, \ldots, \bar{\Delta}_n) \ (l),$$

oder

$$g(\Delta_1, \Delta_2, \ldots, \Delta_n) \equiv \sum_{i=1}^{n-1} (\Delta_1 x_1^{(i)} + \Delta_2 x_2^{(i)} + \cdots + \Delta_n x_n^{(i)}) \, h_i(\Delta_1, \Delta_2, \ldots, \Delta_n) \ (l). \ —$$

Wir beweisen nun einen dritten Hilfssatz. Es sei $\mathfrak{G}(a)$ eine Untergruppe von $\mathfrak{G}$ vom Index l, bestimmt durch die Kongruenz

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n \equiv 0(l).$$

Wie früher gezeigt wurde, ist dann

$$\mathfrak{C}(a) = \{T_{ik}^{a_j} T_{kj}^{a_i} T_{ji}^{a_k}, \ T_{ik}^{\Delta_1 x_1^{(j)} + \Delta_2 x_2^{(j)} + \cdots + \Delta_n x_n^{(j)}}\},$$

wenn

$$a_1 x_1^{(j)} + a_2 x_2^{(j)} + \cdots + a_n x_n^{(j)} \equiv 0(l).$$

Wir behaupten den

Hilfssatz 3. *Die symbolischen Potenzen*

$$(T_{ik}^{a_j} T_{kj}^{a_i} T_{ji}^{a_k})^{\Delta_r}, \qquad (r = 1, 2, \ldots, n),$$

können durch symbolische Potenzprodukte der Kommutatoren

$$T_{ik}^{\Delta_1 x_1^{(j)} + \Delta_2 x_2^{(j)} + \cdots + \Delta_n x_n^{(j)}}$$

ersetzt werden.

Beweis. Wir unterscheiden zwei Fälle:

1. r sei mit einer der Zahlen i, k, j identisch, etwa $r = i$. Es ist dann wegen der in § 1 behandelten Relationen II

$$(T_{ik}^{a_j} T_{kj}^{a_i} T_{ji}^{a_k})^{\Delta_i} = T_{ik}^{\Delta_i a_j - \Delta_j a_i} T_{ji}^{\Delta_i a_k - \Delta_k a_i},$$

also wegen Hilfssatz 2 durch die $T_{ik}^{\Delta_1 x_1^{(j)} + \Delta_1 x_2^{(j)} + \cdots + \Delta_n x_n^{(j)}}$ darstellbar.

2. $r \neq i, k, j$. Mit Hilfe der Relationen

$$T_{kj}^{\Delta_r} T_{jr}^{\Delta_k} T_{rk}^{\Delta_j} = E,$$

$$T_{ji}^{\Delta_r} T_{ir}^{\Delta_j} T_{rj}^{\Delta_i} = E,$$

$$T_{ik}^{\Delta_r} T_{kr}^{\Delta_i} T_{ri}^{\Delta_k} = E$$

erhalten wir

$$(T_{ik}^{a_j} T_{kj}^{a_i} T_{ji}^{a_k})^{\Delta_r} = T_{kr}^{\Delta_j a_i - \Delta_i a_j} T_{ri}^{\Delta_j a_k - \Delta_k a_j} T_{jr}^{\Delta_i a_k - \Delta_k a_i},$$

so daß zufolge Hilfssatz 2 die Behauptung wieder bewiesen ist.

Hilfssatz 4. *Ist $f(x_1, x_2, \ldots, x_n)$ ein ganzzahliges Polynom, dessen Grad in jeder Veränderlichen die Zahl $l-1$ nicht übersteigt und welches mod. l nicht identisch verschwindet, so gibt es ein spezielles Wertesystem $\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n$, so daß*

$$f(\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n) \not\equiv 0(l).$$

Beweis. Für eine Veränderliche ist der Satz eine unmittelbare Folge der Tatsache, daß in dem endlichen Körper der Restklassen mod. l eine Gleichung vom Grade $l-1$ höchstens $l-1$ Wurzeln haben kann. Wir führen daher den Beweis mit Hilfe vollständiger Induktion nach der Zahl der Veränderlichen. Wir ordnen $f(x_1, x_2, \ldots, x_n)$ nach der Veränderlichen x_n,

$$f(x_1, x_2, \ldots, x_n) = x_n^{l-1} \varphi_1(x_1, x_2, \ldots, x_{n-1}) + \cdots + x_n \varphi_{l-1}(x_1, x_2, \ldots, x_{n-1}) + \varphi_l(x_1, x_2, \ldots, x_{n-1}).$$

Dann bestimmen wir die Zahlen $\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_{n-1}$ so, daß mindestens eines der $\varphi_i(\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_{n-1}) = \bar{\varphi}_i \not\equiv 0(l)$ wird. Nach Induktionsvoraussetzung ist dies sicherlich möglich. Die Funktion

$$f(\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_{n-1}, x_n) = x_n^{l-1} \bar{\varphi}_1 + \cdots + x_n \bar{\varphi}_{l-1} + \bar{\varphi}_l$$

verschwindet nicht identisch, und es gibt daher einen Wert $\bar{x}_n$, so daß $f(\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n)$ einen nicht durch l teilbaren Wert annimmt.

§ 3.

Wir führen den Beweis von Satz II zunächst für den Fall, daß die Zahl der Basisklassen $n = 3$ ist.

Die Klassengruppe des Grundkörpers sei also

$$c_1^{x_1} c_2^{x_2} c_3^{x_3}, \qquad (0 \leqq x_i < l).$$

Die Relativgruppe des zweiten Klassenkörpers lautet

$$\mathfrak{G} = S_1^{x_1} S_2^{x_2} S_3^{x_3} \mathfrak{C}, \qquad (0 \leqq x_i < l),$$

wobei S_i die der Klasse c_i eindeutig zugeordnete Substitution ist [1]). Dabei hat die Kommutatorgruppe $\mathfrak{C}$ nach unserer Annahme folgende Gestalt: $\mathfrak{C}$ wird symbolisch erzeugt von den Kommutatoren T_{12}, T_{13}, T_{23}, und es ist

$$T_{ik}^{l} = E,$$

$$T_{ik}^{\Delta_{j_1} \Delta_{j_2} \cdots \Delta_{j_{l-1}}} = E.$$

Außer den Potenzprodukten dieser beiden Relationen besitze die Kommutatorgruppe nur noch die Relation

[1]) Siehe Artin, Hamburger Sem. Abhandlungen 5, S. 361.

$$T_{123} : T_{12}^{\Delta_3} T_{23}^{\Delta_1} T_{31}^{\Delta_2} = E.$$

Die Stammrelationen seien

$$S_j^l = \prod_{(ik=12,23,31)} T_{ik}^{g_{ik}^{(j)}}, \qquad (j = 1, 2, 3), \tag{1}$$

und die $g_{ik}^{(j)}$ ganzzahlige Formen in den $\Delta_1, \Delta_2, \Delta_3$ vom Grade $l-2$.

Wir wollen nun zeigen, daß sich unter diesen Voraussetzungen zu einer geeignet gewählten Basis $\bar{c}_1, \bar{c}_2, \bar{c}_3$ drei relativ zyklische unverzweigte Oberkörper k_1, k_2, k_3 angeben lassen, so daß $\bar{c}_i$ die einzige Klasse von k ist, die in k_i Hauptklasse wird.

$k(y) = k(y_1, y_2, y_3)$ sei ein unverzweigter Oberkörper von k vom Relativgrad l, bestimmt durch die Kongruenz

$$y_1 x_1 + y_2 x_2 + y_3 x_3 \equiv 0(l)\ ^{1}).$$

Sind

$$x_1^{(i)},\ x_2^{(i)},\ x_3^{(i)}, \qquad (i = 1, 2),$$

zwei unabhängige Lösungen dieser Kongruenz, so ist

$$\mathfrak{G}(y) = \{S_1^{x_1^{(i)}} S_2^{x_2^{(i)}} S_3^{x_3^{(i)}},\quad (i = 1, 2),\ \mathfrak{C}\}$$

und

$$\mathfrak{C}(y) = \{T_{12}^{y_3} T_{23}^{y_1} T_{31}^{y_2},\quad T_{ik}^{\Delta_1 x_1^{(j)} + \Delta_2 x_2^{(j)} + \Delta_3 x_3^{(j)}},\ (j = 1, 2)\}.$$

Jeder Klasse von $k(y)$ wird mittels der Frobeniusschen Kongruenz ein Element der Gruppe $\mathfrak{G}(y) / \mathfrak{C}(y)$ zugeordnet. Der Hauptklasse und nur dieser entsprechen die Elemente der Gruppe $\mathfrak{C}(y)$. Betrachten wir die Elemente, die den Klassen des Grundkörpers k in $k(y)$ entsprechen [2]): es ist dabei zwischen denjenigen Klassen von k zu unterscheiden, die in $k(y)$ zerfallen, und denjenigen, die unzerlegt bleiben. Ist c_i eine Basisklasse von k und S_i die ihr entsprechende Substitution, so entspricht der Klasse c_i in $k(y)$, wenn sie dort zerfällt, die Substitution

$$S_i^{1 + s_k + \cdots + s_k^{l-1}},$$

wobei c_k eine beliebige, in $k(y)$ nicht zerfallende Klasse ist. Da

$$1 + S_k + \cdots + S_k^{l-1} \equiv (S_k - 1)^{l-1}(l),$$

ist

$$S_i^{1 + s_k + \cdots + s_k^{l-1}} = S_i^l\, T_{ik}^{\Delta_k^{l-2}}\, \mathfrak{C}(y).$$

Bleibt c_i dagegen unzerlegt, so wird ihr in $k(y)$ die Substitution

$$S_i^l$$

zugeordnet.

Verstehen wir unter dem Symbol [3])

$$y_{i_1 i_2 \cdots i_r}$$

die Zahl

$$(1 - y_{i_1}^{l-1})(1 - y_{i_2}^{l-1}) \cdots (1 - y_{i_r}^{l-1}),$$

so entspricht der Klasse c_1 im Körper $k(y)$ die Substitution

$$S_1^l\, T_{12}^{\Delta_2^{l-2} y_{11}}\, T_{13}^{\Delta_3^{l-2} y_{11}}. \tag{2}$$

Die den Klassen c_2 und c_3 entsprechenden Substitutionen erhalten wir durch zyklische

---

[1]) Siehe S. 195.

[2]) Siehe Artin, Hamburger Sem. Abhandlungen 7, S. 46.

[3]) Für das Symbol $y_{i_1 i_2 \cdots i_r}$ gelten die folgenden einfachen Beziehungen: $y_{i_1} y_{i_1 i_2 \cdots i_r} \equiv 0(l)$, $y_{12 \cdots n} \equiv 0(l)$, $y_{i_1 i_2 \cdots i_r} \cdot y_{k_1 k_2 \cdots k_s} = y_{i_1 i_2 \cdots i_r k_1 k_2 \cdots k_s}$.

Vertauschung. Da dem Produkt der Klassen das Produkt der Substitutionen entspricht, wird einer beliebigen Klasse $c_1^{u_1} c_2^{u_2} c_3^{u_3}$ ein symbolisches Potenzprodukt

$$T_{12}^{h_{12}(\Delta_1, \Delta_2, \Delta_3)} T_{23}^{h_{23}(\Delta_1, \Delta_2, \Delta_3)} T_{31}^{h_{31}(\Delta_1, \Delta_2, \Delta_3)} \tag{3}$$

zugeordnet, wobei die Exponenten h_{ik} wieder Formen vom Grade $l-2$ sind, die aus den Beziehungen (1) und (2) zu entnehmen sind. Soll die Klasse $c_1^{u_1} c_2^{u_2} c_3^{u_3}$ in $k(y)$ zur Hauptklasse werden, so muß die ihr entsprechende Substitution (3) ein Element von $\mathfrak{C}(y)$ sein. Für $l=2$ ist

$$\mathfrak{C}(y) = \{T_{12}^{y_3} T_{23}^{y_1} T_{31}^{y_2}\},$$

also muß es in diesem Falle eine Zahl v geben, so daß

$$T_{12}^{h_{12}} T_{23}^{h_{23}} T_{31}^{h_{31}} = (T_{12}^{y_3} T_{23}^{y_1} T_{31}^{y_2})^v.$$

Ist $l>2$, so muß das Element (3), wenn es in $\mathfrak{C}(y)$ liegen soll, sich nach Hilfssatz 3 als symbolisches Potenzprodukt der $T_{ik}^{\Delta_1 x_1^{(j)} + \Delta_2 x_2^{(j)} + \Delta_3 x_3^{(j)}}$ und des Elementes T_{123} darstellen lassen. Es müssen also Formen vom Grad $l-3$ existieren:

$$q_{ik}^{(j)}(\Delta_1, \Delta_2, \Delta_3), \quad (i, k = 1, 2, 3,\ i \neq k;\ j = 1, 2), \text{ und } q(\Delta_1, \Delta_2, \Delta_3),$$

so daß

$$T_{12}^{h_{12}(\Delta)} T_{13}^{h_{13}(\Delta)} T_{23}^{h_{23}(\Delta)} T_{123}^{q(\Delta)} = \prod_{i \neq k} T_{ik}^{(\Delta_1 x_i' + \Delta_2 x' + \Delta_3 x_3') q_{ik}'(\Delta) + (\Delta_1 x_i'' + \Delta_2 x_i'' + \Delta_3 x_3'') q_{ik}''(\Delta)}.$$

Setzen wir $q(y_1, y_2, y_3) = v$, so liefern diese Beziehungen für $l=2$ unmittelbar, für $l>2$ nach Hilfssatz 2 das Bestehen der drei Kongruenzen

$$h_{ik}(y_1, y_2, y_3) + y_j v \equiv 0(l), \qquad (i \neq k,\ i \neq j,\ k \neq j).$$

Ordnen wir diese Kongruenzen nach den Größen u_1, u_2, u_3, v, so erhalten wir das folgende Kongruenzensystem:

$$\begin{array}{l|l}
u_1 & (y_{11} y_2^{l-2} + g_{12}^{(1)}) + u_2(-y_{23} y_1^{l-2} + g_{12}^{(2)}) + u_3 g_{12}^{(3)} + v y_3 \equiv 0(l) \\
u_1 g_{23}^{(1)} & + u_2 (y_{22} y_3^{l-2} + g_{23}^{(2)}) + u_3(-y_{31} y_2^{l-2} + g_{23}^{(3)}) + v y_1 \equiv 0(l) \\
u_1(-y_{12} y_3^{l-2} + g_{31}^{(1)}) + u_2 g_{31}^{(2)} & + u_3 (y_{33} y_1^{l-2} + g_{31}^{(3)}) + v y_2 \equiv 0(l).
\end{array}$$

Dabei verstehen wir unter $g_{ik}^{(j)}$ die Zahl $g_{ik}^{(j)}(y_1, y_2, y_3)$.

Soll die Klasse $c_1^{u_1} c_2^{u_2} c_3^{u_3}$ in $k(y)$ in die Hauptklasse übergehen, so muß gelten:

$$u_1 : u_2 : u_3 = D_1(y_1, y_2, y_3) : D_2(y_1, y_2, y_3) : D_3(y_1, y_2, y_3).$$

Dabei ist

$$D_1(y_1, y_2, y_3) = y_{23} y_1^{l-3} - y_{33} g_{12}^{(2)} + y_{22} g_{31}^{(3)} + y_1 G_{(31,12)}^{(2,3)} + y_2 G_{(12,23)}^{(2,3)} + y_3 G_{(23,31)}^{(2,3)}.$$

Unter $G_{(i_1 i_2, j_1 j_2)}^{(i,k)}$ werde dabei die aus den Spalten $i_1 i_2$, $j_1 j_2$ und den Zeilen i, k gebildete zweizeilige Unterdeterminante der Determinante $|g_{ik}^{(j)}(y_1, y_2, y_3)|$ verstanden. Der Wert von $D_2(y_1, y_2, y_3)$ und $D_3(y_1, y_2, y_3)$ ergibt sich aus $D_1(y_1, y_2, y_3)$ durch Indexvertauschungen. In $k(y)$ geht genau eine Klasse in die Hauptklasse über, wenn $D_1(y)$, $D_2(y)$, $D_3(y)$ nicht gleichzeitig durch l teilbar sind. Die Polynome $D_i(y_1, y_2, y_3)$ verschwinden mod. l nicht identisch. $D_1(y)$ enthält z. B. den Term $y_2^{l-1} y_3^{l-1} y_1^{l-3}$ mit dem Koeffizienten 1. Ebenso verschwindet auch $D_1(1, y_2, y_3)$ nicht identisch mod. l. Betrachten wir die Determinante

$$|D_j(y_1^{(i)}, y_2^{(i)}, y_3^{(i)})|, \qquad (i, j = 1, 2, 3),$$

gebildet aus den Polynomen $D_j(y)$ für drei verschiedene Körper $k(y^{(i)})$, $(i = 1, 2, 3)$. Es sei $y_i^{(i)} = 1$, $(i = 1, 2, 3)$ [1]). Diese Determinante ist ein mod. l nicht identisch verschwindendes Polynom in sechs Veränderlichen. Nach Hilfssatz 4 gibt es also Zahlen $y_2^{(1)}, y_3^{(1)}, y_1^{(2)}, y_3^{(2)}, y_1^{(3)}, y_2^{(3)}$, so daß die Determinante eine nicht durch l teilbare Zahl wird. Setzen wir nun

[1]) Diese Festsetzung wird getroffen, um Lösungen $y_1^{(i)} \equiv y_2^{(i)} \equiv \cdots \equiv y_n^{(i)} \equiv 0(l)$ zu vermeiden.

$$u_1^{(i)} : u_2^{(i)} : u_3^{(i)} = D_1(y_1^{(i)}, y_2^{(i)}, y_3^{(i)}) : D_2(y_1^{(i)}, y_2^{(i)}, y_3^{(i)}) : D_3(y_1^{(i)}, y_2^{(i)}, y_3^{(i)}),$$

so sind die drei Klassen

$$c_1^{u_1^{(i)}}\, c_2^{u_2^{(i)}}\, c_3^{u_3^{(i)}}, \qquad (i = 1, 2, 3),$$

unabhängig, also als Basisklassen brauchbar. Wir haben somit die Existenz von drei Klassen und drei verschiedenen Körpern $k(y)$ nachgewiesen, so daß erstens jeder Körper genau eine Klasse in die Hauptklasse führt, und zweitens diese drei Klassen eine Basis für die Klassengruppe des Grundkörpers bilden.

§ 4.

Für allgemeines $n > 3$ läßt sich der Beweis in der folgenden Weise erbringen[1]): Ist die Klassengruppe in k

$$c_1^{x_1}\, c_2^{x_2} \cdots c_n^{x_n}, \qquad (0 \leqq x_i < l),$$

so ist die zugehörige zweistufige Gruppe von der Form

$$\mathfrak{G} = S_1^{x_1}\, S_2^{x_2} \cdots S_n^{x_n}\, \mathfrak{C}, \qquad (0 \leqq x_i < l).$$

Ein „vollständiges System" von Relationen für $\mathfrak{C}$ sei

$$T_{ik}^{l} = E,$$
$$T_{ik}^{\Delta_{i_1}\Delta_{i_2}\cdots\Delta_{i_{l-1}}} = E,$$
$$T_{ik}^{\Delta_j}\, T_{kj}^{\Delta_i}\, T_{ji}^{\Delta_k} = E.$$

Die Stammrelationen seien

$$(1) \qquad S_j^{l} = \Pi\, T_{ik}^{g_{ik}^{(j)}(\Delta_1, \Delta_2, \ldots, \Delta_n)}, \qquad (j = 1, 2, \ldots, n),$$

die $g_{ik}^{(j)}(\Delta_1, \Delta_2, \ldots, \Delta_n)$ Formen vom Grade $l - 2$.

Dabei werden diese Produkte erstreckt über die ersten $\binom{n}{2}$ Ziffernpaare ik, welche aus $1\,j$, $\left(j = 2, 3, \ldots, \left[\frac{n+1}{2}\right]\right)$, durch zyklische Vertauschung hervorgehen. Auch im folgenden wird diese Numerierung stets vorausgesetzt, wenn nichts anderes hervorgehoben wird.

In $k(y_1, y_2, \ldots, y_n)$ entspricht der Basisklasse c_1 die Substitution

$$(2) \qquad S_1^{l}\, T_{12}^{\Delta_2^{l-2} y_{11}}\, T_{13}^{\Delta_3^{l-2} y_{12}}\, T_{14}^{\Delta_4^{l-2} y_{123}} \ldots T_{1n}^{\Delta_n^{l-2} y_{12\cdots(n-1)}}.$$

Den Basisklassen $c_2, c_3, \ldots, c_n$ entsprechen die daraus durch zyklische Vertauschung der Indizes hervorgehenden Substitutionen. Daher entspricht jeder Klasse $c_1^{u_1}\, c_2^{u_2} \cdots c_n^{u_n}$ in $k(y)$ eine Substitution

$$(3) \qquad \Pi\, T_{ik}^{h_{ik}(\Delta_1, \Delta_2, \ldots, \Delta_n)},$$

wobei die $h_{ik}(\Delta)$ Formen vom Grade $l - 2$ sind, die aus den Beziehungen (1) und (2) hervorgehen. Soll eine Klasse von k in $k(y)$ zur Hauptklasse werden, so muß die ihr entsprechende Substitution (3) in $\mathfrak{C}(y)$ liegen. Es muß also dann für $l = 2$ Zahlen v_{ikj} geben, so daß

$$\Pi\, T_{ik}^{h_{ik}} \prod_{i \neq k \neq j \neq i} (T_{ik}^{y_j}\, T_{kj}^{y_i}\, T_{ji}^{y_k})^{v_{ikj}} = E.$$

Für $l > 2$ läßt sich $\Pi\, T_{ik}^{h_{ik}(\Delta)}$, multipliziert mit einem Potenzprodukt der T_{ikj}, $T_{ikj}^{q_{ikj}(\Delta_1, \Delta_2, \ldots, \Delta_n)}$, nach Hilfssatz 3 als Potenzprodukt der $T_{ik}^{\Delta_1 x_1^{(j)} + \Delta_2 x_2^{(j)} + \cdots + \Delta_n x_n^{(j)}}$ darstellen.

---

[1]) Für $n = 2$ ist der Beweis von Satz I und II wesentlich einfacher als für $n > 2$; wir wollen uns daher auf diesen letzteren Fall beschränken.

Wir setzen $q_{ikj}(y_1, y_2, \ldots, y_n) = v_{ikj}$ und erhalten nach Hilfssatz 2 wieder das Bestehen von $\binom{n}{2}$ linearen homogenen Kongruenzen:

$$h_{ik}(y_1, y_2, \ldots, y_n) - y_{i+1}\, v_{ik,i+1} - y_{i+2}\, v_{ik,i+2} - \cdots - y_{k-1}\, v_{ik,k-1} + y_{k+1}\, v_{ik,k+1} + \cdots + y_{i-1}\, v_{ik,i-1} \equiv 0(l).$$

Ordnen wir diese Kongruenzen nach $u_1, u_2, \ldots, u_n$ und den Größen v_{ikj}, so erhalten wir das System:

$$u_1(y_{12\ldots(k-1)}\, y_k^{l-2} + g_{1k}^{(1)}) + u_2\, g_{1k}^{(2)} + \cdots + u_{k-1}\, g_{1k}^{(k-1)} + u_k(-y_{k(k+1)\ldots n}\, y_1^{l-2} + g_{1k}^{(k)}) + u_{k+1}\, g_{1k}^{(k+1)} + \cdots + u_n\, g_{1k}^{(n)} - v_{1k2}\, y_2 - v_{1k3}\, y_3 - \cdots - v_{1k,k-1}\, y_{k-1} + v_{1k,k+1}\, y_{k+1} + v_{1k,k+2}\, y_{k+2} + \cdots + v_{1kn}\, y_n \equiv 0\ (l),$$

$\left(k = 2, 3, \ldots, \left[\frac{n+1}{2}\right]\right)$, und die sämtlichen aus diesen Kongruenzen durch zyklische Vertauschung der Indizes hervorgehenden.

Die Matrix dieses Systems hat also $\binom{n}{2}$ Zeilen und $n + \binom{n}{3}$ Spalten. Da von den letzten $\binom{n}{3}$ Spalten nach Hilfssatz 1 nur $\binom{n-1}{2}$ linear unabhängig sind, haben wir zwar formal $n + \binom{n}{3}$ Unbekannte, um die in die Hauptklasse übergehenden Klassen zu bestimmen, doch sind nur $n + \binom{n-1}{2} = \binom{n}{2} + 1$ wesentliche Unbekannte darunter. Sind nicht alle $\binom{n}{2}$-zeiligen Determinanten der Matrix, die genau $n-1$ der ersten n Spalten enthalten, mod. l verschwindende Polynome in den $y_1, y_2, \ldots, y_n$ so gibt es Körper $k(y_1, y_2, \ldots, y_n)$, in denen nur je eine Klasse Hauptklasse wird. Wir erhalten u_1 als Linearform

$$u_1 = \lambda_1 \Delta_1 + \lambda_2 \Delta_2 + \cdots$$

der Determinanten Δ_i, die bei Weglassung der ersten und je $\binom{n}{3} - \binom{n-1}{2} = \binom{n-1}{3}$ der letzten $\binom{n}{3}$ Spalten der Matrix hervorgehen. Wir brauchen nur zu zeigen, daß nicht sämtliche Δ_i identisch mod. l verschwinden können. Nach Hilfssatz 4 können wir dann den y_i und λ_i solche Werte erteilen, daß auch u_1 nicht durch l teilbar wird. Das Entsprechende gilt natürlich für die weiteren Unbekannten $u_2, u_3, \ldots, u_n$. Wir zeigen nun im folgenden, daß die Determinante Δ_1, die bei Weglassung der ersten Spalte der Matrix und aller jener Spalten unter den letzten $\binom{n}{3}$, die y_1 nicht enthalten, entsteht, nicht identisch verschwindet:

Die ersten $n-1$ Spalten der Determinante Δ_1 nennen wir die „Anfangsspalten", die $\binom{n-1}{2}$ letzten die „Endspalten". In der T_{ik} entsprechenden Zeile $(i\,k)$ stehen in den Anfangsspalten die $g_{ik}^{(j)}$, $(j = 2, 3, \ldots, n)$, und in der i-ten Spalte [1]) außerdem der Term

$$y_{i,i+1,\ldots,k-1}\, y_k^{l-2},$$

in der k-ten Spalte außerdem der Term

$$y_{k,k+1,\ldots,i-1}\, y_i^{l-2}.$$

[1]) Unter der j-ten Spalte wird die zu $g_{ik}^{(j)}$ gehörige Anfangsspalte verstanden.

Für die Endspalten gilt:

In jeder Spalte treten außer y_1 noch zwei weitere y_i auf; sonst enthält die Spalte lauter Nullen. In der Zeile $(i\,k)$ kommen, wenn $i, k \neq 1$, außer y_1 nur Nullen vor. Ist dagegen $i = 1$, so treten in der betreffenden Zeile genau $n-2$ der y_i auf. Wir wollen Δ_1 als Summe der i-zeiligen Determinanten, $(i = 0, 1, \ldots, n-1)$, darstellen, die sich aus den $g_{ik}^{(j)}$ bilden lassen, mit Koeffizienten, die von den $y_1, y_2, \ldots, y_n$ abhängen.

Betrachten wir zuerst das von den $g_{ik}^{(j)}$ freie Glied von Δ_1; wir erhalten es, indem wir alle $g_{ik}^{(j)} = 0$ setzen, als Determinante, deren erste Spalte die folgenden Elemente enthält:

$$y_{23\ldots n}\, y_1^{l-2},\ y_{23\ldots(n-1)}\, y_n^{l-2},\ y_{23\ldots(n-2)}\, y_{n-1}^{l-2}, \ldots, y_{22}\, y_3^{l-2}, 0, \ldots, 0.$$

Die weiteren $n-2$ Anfangsspalten sind analog gebaut. Also ist die erste Spalte durch y_{22}, die zweite durch y_{33}, usw., die $(n-1)$-te Spalte durch y_{nn} teilbar, so daß wir aus der ganzen Determinante den Faktor $y_{23\ldots n}$ herausheben können, und in dem übrigbleibenden Polynom alle $y_i \neq y_1$ durch 0 ersetzen dürfen, da ja $y_i\, y_{ii} \equiv 0\ (l)$ gilt. Dann bleiben aber in den Anfangsspalten nur die Terme y_1^{l-2} übrig, und zwar so, daß in jeder der $n-1$ Spalten je ein Term y_1^{l-2} steht, und sich die ganze Determinante abgesehen vom Vorzeichen in die Form bringen läßt:

$$\left|\begin{array}{ccccccc}
y_1^{l-2} & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\
0 & y_1^{l-2} & & & & & \vdots \\
\vdots & & \ddots & & & & \vdots \\
\vdots & & & \ddots & & & \vdots \\
\vdots & & & & y_1^{l-2} & & \vdots \\
\vdots & & & & & y_1 & \vdots \\
\vdots & & & & & & \vdots \\
\vdots & & & & & & \vdots \\
0 & \cdots & \cdots & \cdots & \cdots & \cdots & y_1
\end{array}\right\}\begin{array}{l} \left.\begin{array}{l}\\\\\\\\\\\\\end{array}\right\} n-1 \\ \left.\begin{array}{l}\\\\\\\\\end{array}\right\} \binom{n-1}{2} \end{array}.$$

Das von den $g_{ik}^{(j)}$ freie Glied lautet daher

$$G_0 = \pm\, y_{23\ldots n}\, y_1^{(l-2)(n-1)+\binom{n-1}{2}}.$$

Wenn wir nun zeigen können, daß außer in G_0 kein Term $y_1^{(l-2)(n-1)+\binom{n-1}{2}} y_2^{l-1} y_3^{l-1} \cdots y_n^{l-1}$ auftritt, dann ist die Behauptung, daß nämlich Δ_1 nicht identisch verschwindet, bewiesen.

Zunächst beweisen wir den folgenden Satz über die Koeffizienten der aus den $g_{ik}^{(j)}$ gebildeten Unterdeterminanten:

1. Für $k = 1, 2, \ldots, n-1$ verschwinden in Δ_1 die Koeffizienten aller k-zeiligen Determinanten der $g_{ik}^{(j)}$, $\binom{i, k = 1, 2, \ldots, n}{j = 2, 3, \ldots, n}$, mit Ausnahme der folgenden:

$$\begin{pmatrix} j_1 & j_2 & \cdots & j_k \\ 1\,j_1 & i_2 j_2 & \cdots & i_k j_k \end{pmatrix}\ ^{1}).$$

Dabei ist $j_\varrho \neq j_\sigma$, wenn $\varrho \neq \sigma$, und die i_α, die nicht paarweise verschieden sein müssen, sind aus der Folge $1, j_1, \ldots, j_k$ so gewählt, daß die $i_\alpha\, j_\alpha$ keinen Zyklus enthalten.

2. Der Koeffizient dieser Determinanten ist dann aber

$$G_{(1\,j_1,\ i_2 j_2,\ \ldots,\ i_k j_k)}^{(j_1,\ j_2,\ \ldots,\ j_k)} = \pm\, y_1^{(l-2)(n-k-1)+\binom{n-1}{2}-\sum_{j=1}^{k}\varrho_j}\, y_{j_1}^{\varrho_1} y_{j_2}^{\varrho_2} \cdots y_{j_k}^{\varrho_k} y_{r_1 r_2 \ldots r_{n-k}}.$$

Die Indizes $r_1, r_2, \ldots, r_{n-k}$ sind paarweise verschiedene Zahlen aus der Reihe $2, 3, \ldots, n$, die sämtlich von den Zahlen $j_1, j_2, \ldots, j_k$ verschieden sind.

---

[1]) Unter $\begin{pmatrix} \alpha_1 & \alpha_2 & \cdots \alpha_r \\ \beta_1\gamma_1 & \beta_2\gamma_2 & \cdots \beta_r\gamma_r \end{pmatrix}$ wird eine r-zeilige Determinante der Matrix $(g_{ik}^{(j)})$ verstanden, deren Elemente den Zeilen $\alpha_1, \alpha_2, \ldots, \alpha_r$ und den Spalten $\beta_1\gamma_1, \beta_2\gamma_2, \ldots, \beta_r\gamma_r$ in der angegebenen Reihenfolge entnommen sind.

Setzen wir

$$\delta_{rs} = 0, \quad \text{wenn} \quad r \neq s,$$
$$= 1, \quad \text{wenn} \quad r = s,$$

so ist

$$\varrho_1 = \sum_{\alpha=2}^{k} \delta_{j_1 i_\alpha}$$
$$\varrho_2 = \sum_{\alpha=2}^{k} \delta_{j_2 i_\alpha}$$
$$\cdots\cdots\cdots$$
$$\varrho_k = \sum_{\alpha=2}^{k} \delta_{j_k i_\alpha}.$$

Wir bringen zunächst den Beweis der Behauptung 2. Wir denken uns die Numerierung so gewählt, daß $j_\alpha = \alpha + 1$, $(\alpha = 1, 2, \ldots, k)$, ist. Wir betrachten also den Koeffizienten der Determinante

$$\begin{pmatrix} 2 & 3 & \ldots & k+1 \\ 1\,2 & i_2\,3 & \ldots & i_k\,k+1 \end{pmatrix},$$

wobei die i_α der Folge $1, 2, \ldots, k+1$ entnommen sind.

Wir können aus den Anfangsspalten den Faktor $y_{k+2,k+3,\ldots,n}$ herausheben, daher im übrig bleibenden Polynom $y_{k+2}, y_{k+3}, \ldots, y_n$ durch Null ersetzen. Ist $k < n-2$, so enthält die Endspalte $v_{1,n-1,n}$ nach diesem Prozeß nur mehr das Element y_1, sonst Nullen. Es ist also der ganze Koeffizient in diesem Falle durch y_1 teilbar. Ist $k = n-2$ oder $n-1$, so gibt es, da $n > 3$ angenommen wurde, stets eine Zeile (rs), $r, s \neq 1$, die das Element y_1 und sonst lauter Nullen enthält. Der Koeffizient ist also auf jeden Fall durch y_1 teilbar. Ersetzen wir im nun übrig bleibenden Polynom y_{11} durch Null, so bleiben in den Anfangsspalten nur die mit y_1^{l-2} multiplizierten Terme. Die mit $y_2^{l-1}, y_3^{l-1}, \ldots, y_{k+1}^{l-1}$ multiplizierten Terme verschwinden nämlich, da sie auch den Faktor y_{11} hatten, die mit $y_{k+2}^{l-2}, y_{k+3}^{l-2}, \ldots, y_n^{l-2}$ multiplizierten sind durch l teilbar wegen des Faktors $y_{k+2,\ldots,n}$. Also können wir aus den Anfangsspalten noch $y_1^{(l-2)(n-k-1)}$ herausheben und die entsprechenden Spalten und Zeilen streichen. Wir erhalten also als Koeffizienten $\pm y_1^{(l-2)(n-k-1)}$, multipliziert mit einer Unterdeterminante, die nur aus Endspalten besteht. Sind alle $i_\alpha = 1$, $\alpha = 2, 3, \ldots, k$, so liefern diese Endspalten die Determinante

$$y_1^{\binom{n-1}{2}} = \left.\begin{vmatrix} y_1 & \cdots & \cdots & 0 \\ \cdot & y_1 & & \cdot \\ \cdot & & \cdot & \cdot \\ \cdot & & & \cdot \\ \cdot & & & \cdot \\ 0 & \cdots & \cdots & y_1 \end{vmatrix}\right\} \binom{n-1}{2}.$$

Für diesen Fall ist also die Behauptung 2 bereits vollständig bewiesen. Wir müssen daher noch den Fall behandeln, daß nicht sämtliche $i_\alpha = 1$ sind:

a) Es sei $i_\alpha \neq 1$ und $i_{i_\alpha - 1} = 1$.

In diesem Falle lautet die Spalte $v_{1 i_\alpha (\alpha+1)}$ nicht

$$0 \ldots 0 \; y_1 \; 0 \ldots 0,$$

sondern

$$0 \ldots 0 \; y_{i_\alpha} \; 0 \ldots 0.$$

Es tritt also ein Faktor y_1 weniger auf, während der Faktor y_{i_α} hinzukommt.

b) Es seien einige der von 1 verschiedenen i_α so beschaffen, daß auch $i_{i_\alpha - 1} \neq 1$ ist.

Wir streichen nun zuerst in der aus den Endspalten bestehenden Unterdeterminante die Elemente y_1 und die entsprechenden Zeilen und Spalten. Ebenso heben wir alle jene y_{i_α} heraus, für welche $i_{i_\alpha - 1} = 1$ ist, und streichen die dazu gehörigen Zeilen und

Spalten. Wir verfahren ebenso, wenn ein $i_\alpha = 2$ vorkommt, und auch wenn irgendein $i_\alpha \neq 1, 2$ die Eigenschaft hat, daß $\alpha+1$ nicht auch unter den i_α auftritt. Ist dann die ganze Determinante erschöpft, so ist Behauptung 2 bereits bewiesen. Andernfalls tritt unter den Paaren $i_\alpha(\alpha+1)$ bei geeigneter Numerierung ein Zyklus auf. In diesem Fall verschwindet die Determinante.

Wir führen jetzt den Beweis der Behauptung 1, nämlich, daß die Koeffizienten aller anderen Unterdeterminanten identisch verschwinden.

Wir denken uns auch hier die Numerierung so gewählt, daß die $g_{ik}^{(j)}$ den Spalten $2, 3, \ldots, k+1$ entnommen sind. Der Beweis wird in mehreren Schritten erbracht.

a) Wir zeigen, daß die Determinanten

$$\begin{pmatrix} 2 & 3 & \ldots & k+1 \\ 1\, i_1 & r_2 s_2 & \ldots & r_k s_k \end{pmatrix},$$

$$i_1 \neq 2, 3, \ldots, k+1; \quad r_j, s_j \text{ beliebig},$$

verschwindende Koeffizienten haben. Heben wir nämlich wieder $y_{k+2,\ldots,n}$ und y_1 aus der als Koeffizient auftretenden Determinante heraus und ersetzen wir in der übrigbleibenden Determinante $y_{k+2}, y_{k+3}, \ldots, y_n$ und y_{11} durch 0, so verschwindet die Anfangsspalte i_1.

b) Nun betrachten wir die Koeffizienten der Unterdeterminanten

$$\begin{pmatrix} 2 & 3 & \ldots & k+1 \\ 1\,2 & r_2 s_2 & \ldots & r_k s_k \end{pmatrix},$$

wobei eine der Zahlen r_j, s_j, etwa $r_2 \neq 1, 2, \ldots, k+1$ sei. Wir heben wieder $y_{k+2,\ldots,n}$ und y_1 heraus und ersetzen dann $y_{k+2}, y_{k+3}, \ldots, y_n$ und y_{11} durch 0. Ist $2 \leqq s_2 \leqq k+1$, so ist die Endspalte $v_{1r_2s_2}$ proportional der Anfangsspalte r_2. Da $r_2 > k+1$ vorausgesetzt ist, enthalten nämlich beide Spalten nur in der Zeile $(1\,r_2)$ ein von Null verschiedenes Element. Die Determinante verschwindet also in diesem Falle sicherlich. Ist schließlich $s_2 > k+1$, so besteht die Spalte $v_{1r_2s_2}$ aus lauter Nullen.

c)
$$\begin{pmatrix} 2 & 3 & \ldots & k+1 \\ r_1 s_1 & r_2 s_2 & \ldots & r_k s_k \end{pmatrix},$$

$$r_j, s_j \neq 1, \qquad (j = 1, 2, \ldots, k).$$

Kommt unter r_j, s_j eine Ziffer, etwa r_1, vor, die nicht in der Reihe $2, 3, \ldots, k+1$ enthalten ist, so enthält die Endspalte $v_{1r_1s_1}$ nur y_{s_1}, und zwar in der Zeile $(1\,r_1)$, sonst nur Nullen. Sie ist daher der Anfangsspalte r_1 proportional. Da also der Koeffizient in diesem Falle verschwindet, können wir uns auf die Annahme beschränken, daß sämtliche r_j, s_j der Folge $2, 3, \ldots, k+1$ entnommen sind. Die r_j, s_j, $(j = 1, 2, \ldots, k)$, sind dann k Ziffernpaare, in denen höchstens k verschiedene Ziffern vorkommen. Sie enthalten daher bei geeigneter Anordnung der Paare und der Ziffern eines Paares einen Zyklus [1]). Wir wählen die Numerierung so, daß etwa

$$r_1 s_1, \quad r_2 s_2, \quad r_3 s_3, \ldots, r_{k_1} s_{k_1}, \quad k_1 \leqq k$$

dieser Zyklus sei. Es ist also

$$r_1 = s_{k_1} \quad \text{und}$$
$$r_j = s_{j-1}, \; j = 2, 3, \ldots, k_1.$$

Die Endspalten

$$v_{1r_1s_1}, \quad v_{1r_2s_2}, \ldots, v_{1r_{k_1}s_{k_1}}$$

lauten dann folgendermaßen:

---

[1]) Siehe Ph. Furtwängler, Beweis des Hauptidealsatzes, Hamb. Sem. Abh. 7, S. 34.

Zeile	$v_{1r_1s_1}$	$v_{1r_2s_2}$	. . .	$v_{1r_{k_1-1}s_{k_1-1}}$	$v_{1r_{k_1}s_{k_1}}$
$1\,r_1$	y_{r_2}	0		0	$-y_{r_{k_1}}$
$1\,r_2$	$-y_{r_1}$	y_{r_3}		0	0
$1\,r_3$	0	$-y_{r_3}$		.	.
.	.	0		.	.
.	.	.		0	.
$1\,r_{k_1-1}$	.	.		$y_{r_{k_1}}$	0
$1\,r_{k_1}$	0	0		$-y_{r_{k_1-1}}$	y_{r_1}.

Eine Determinante, welche diese k_1 Spalten enthält, muß identisch verschwinden.

d) Es bleibt noch zu beweisen, daß die Determinanten

$$\begin{pmatrix} 2 & 3 & \dots & k+1 \\ 1\,s_1 & r_2 s_2 & \dots & r_k s_k \end{pmatrix}$$

$$r_j, s_j \leqq k+1, \qquad (j = 1, 2, \dots, k),$$

immer dann verschwindende Koeffizienten haben, wenn wir die Anordnung der Paare und der Ziffern der einzelnen Paare nicht so treffen können, daß

$$s_j = j+1, \quad j = 1, 2, \dots, k.$$

Können wir diese Anordnung nicht erreichen, so muß es einen Index $k_1 \leqq k$ geben, so daß bei geeigneter Numerierung in den Ziffernpaaren

$$1\,s_1, r_2 s_2, \dots, r_{k_1} s_{k_1}$$

höchstens k_1 verschiedene Ziffern auftreten. Dann muß aber wieder unter diesen k_1 Ziffernpaaren ein Zyklus auftreten. Wir unterscheiden nun die beiden Fälle:

α) in diesem Zyklus kommt die Ziffer 1 nicht vor. In diesem Falle zeigen wir wie bei c), daß der Koeffizient verschwindet.

β) die Ziffer 1 kommt in dem Zyklus vor. Der Zyklus laute etwa:

$$1\,s_1,\ r_2 s_2, \dots, r_{k_2-1} s_{k_2-1},\ r_{k_2}\,1,$$

so daß

$$s_{j-1} = r_j, \quad j = 2, 3, \dots, k_2.$$

Wir betrachten nun die Endspalten

$$v_{1r_2r_3},\quad v_{1r_3r_4}, \dots, v_{1r_{k_2-1}r_{k_2}}$$

und erhalten

	$v_{1r_2r_3}$	$v_{1r_3r_4}$	. . .	$v_{1r_{k_2-2}r_{k_2-1}}$	$v_{1r_{k_2-1}r_{k_2}}$
$1\,r_3$	y_{r_3}	$-y_{r_4}$	. . .	0	0
$1\,r_4$	0	y_{r_5}	. . .	0	0
.	.	0		.	.
.	.	.		.	.
.	.	.		0	.
$1\,r_{k_2-2}$	.	.		$y_{r_{k_2-1}}$	0
$1\,r_{k_2-1}$	0	0	. . .	$-y_{r_{k_2-2}}$	$y_{r_{k_2}}$.

Eine Determinante, welche diese $k_2 - 2$ Spalten enthält, verschwindet ebenfalls.

Damit ist auch der Beweis der Behauptung 1 erbracht. Um zu zeigen, daß Δ_1 nicht identisch mod. l verschwindet, haben wir nachzuweisen, daß kein Ausdruck

$$(4) \qquad \begin{pmatrix} j_1 & j_2 & \dots & j_k \\ 1\,j_1 & i_2\,j_2 & \dots & i_k\,j_k \end{pmatrix} G^{(j_1, j_2, \dots, j_k)}_{(1j_1, i_2j_2, \dots, i_kj_k)}$$

mod. l einen Term $y_1^{(l-2)(n-1)+\binom{n-1}{2}} y_2^{l-1} y_3^{l-1} \cdots y_n^{l-1}$ enthält, wenn die j_ϱ paarweise verschieden sind und die i_σ nur Zahlen der Reihe $1, j_1, \dots, j_k$ sind. Es ist dabei

$$G^{(j_1,\ j_2,\ \ldots,\ j_k)}_{(1\,j_1,\ i_2 j_2,\ \ldots,\ i_k j_k)} = \pm\, y_1^{(l-2)(n-k-1)+\binom{n-1}{2}-\sum_1^k \varrho_j}\, y_{r_1 r_2 \ldots r_{n-k}}\, y_{j_1}^{\varrho_1} y_{j_2}^{\varrho_2} \cdots y_{j_k}^{\varrho_k},$$

$$r_\varrho \neq r_\sigma, \quad \text{und} \quad \varrho_i = \sum_{\alpha=2}^{k} \delta_{j_i \alpha_i}.$$

Aus der Definition der Zahlen ϱ_i folgt unmittelbar, daß

$$\sum_{i=1}^{k} \varrho_i \leqq k-1$$

ist. Wir wollen sogar nachweisen, daß das Polynom Δ_1 auch für $y_1 = 1$ in den Veränderlichen $y_2, y_3, \ldots, y_n$ nicht identisch mod. l verschwindet. Dazu haben wir zu zeigen, daß (4) für $y_1 = 1$ keinen Term $y_2^{l-1} y_3^{l-1} \cdots y_n^{l-1}$ enthält:

Die Elemente der Unterdeterminante k-ten Grades

$$\begin{pmatrix} j_1 & j_2 & \cdots & j_k \\ 1 j_1 & i_2 j_2 & \cdots & i_k j_k \end{pmatrix}$$

sind Formen $l-2$-ten Grades in den $y_1, y_2, \ldots, y_n$. Für $y_1 = 1$ hat daher jeder ihrer Terme die Gestalt

$$a \cdot y_2^{a_{21}+a_{22}+\cdots+a_{2k}} \cdots y_n^{a_{n1}+a_{n2}+\cdots+a_{nk}},$$

wo a eine ganze Zahl ist und $\sum_{i=2}^{n} a_{ij} \leqq l-2$, $(j = 1, 2, \ldots, k)$.

Soll (4) einen Term $y_2^{l-1} y_3^{l-1} \cdots y_n^{l-1}$ enthalten, so muß einmal identisch gelten:

$$y_{j_1}^{\varrho_1+a_{j_1 1}+a_{j_1 2}+\cdots+a_{j_1 k}}\, y_{j_2}^{\varrho_2+a_{j_2 1}+a_{j_2 2}+\cdots+a_{j_2 k}} \cdots y_{j_k}^{\varrho_k+a_{j_k 1}+a_{j_k 2}+\cdots+a_{j_k k}}$$
$$\equiv y_{j_1}^{l-1} y_{j_2}^{l-1} \cdots y_{j_k}^{l-1}\ (l).$$

Daraus würde das Bestehen der Gleichungen

$$\begin{aligned} \varrho_1 + a_{j_1 1} + a_{j_1 2} + \cdots + a_{j_1 k} &= l-1 \\ \varrho_2 + a_{j_2 1} + a_{j_2 2} + \cdots + a_{j_2 k} &= l-1 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots & \\ \varrho_k + a_{j_k 1} + a_{j_k 2} + \cdots + a_{j_k k} &= l-1 \end{aligned} \tag{5}$$

folgen. Dieses System von Gleichungen führt aber zu einem Widerspruch gegen die Beziehungen

$$\sum_{i=1}^{k} \varrho_i \leqq k-1 \qquad \text{und}$$

$$\sum_{i=1}^{k} a_{j_i r} \leqq l-2, \qquad (r = 1, 2, \ldots, k).$$

Denn addieren wir die k Gleichungen (5), so ergeben die linken Seiten zufolge der obigen Ungleichungen einen Wert

$$\leqq k-1+k(l-2) = k(l-1)-1,$$

die rechten Seiten aber ergeben

$$k(l-1).$$

Wir sind also zu einem Widerspruch gelangt, aus dem hervorgeht, daß Δ_1 für $y_1 = 1$ nur einen Term $y_2^{l-1} y_3^{l-1} \cdots y_n^{l-1}$ enthält, also nicht identisch verschwindet.

Wir hatten früher die Exponenten $u_1, u_2, \ldots, u_n$ der im Körper $k(y)$ in die Hauptklasse übergehenden Klassen $c_1^{u_1} c_2^{u_2} \cdots c_n^{u_n}$ als Polynome in den $y_1, y_2, \ldots, y_n$ dargestellt, und zwar können wir

$$u_1(y_1, y_2, \ldots, y_n) = \lambda_1 \Delta_1 + \lambda_2 \Delta_2 + \cdots + \lambda_n \Delta_n$$

setzen, wobei Δ_i diejenige Determinante sei, die entsteht, wenn man die erste Spalte der Matrix des Gleichungssystems wegläßt und nur diejenigen der letzten $\binom{n}{2}$ Spalten heranzieht, die das Element y_i enthalten [1]). $u_2, u_3, \ldots, u_n$ lassen sich analog darstellen.

[1]) Aus dem Beweise des Hilfssatzes 1 geht hervor, daß wir bereits mit diesen n Determinanten Δ_i auskommen.

Man erkennt leicht, daß Δ_i, $(i \neq 1)$, aus Δ_1 hervorgeht, wenn man erstens nur diejenigen Unterdeterminanten

$$\begin{pmatrix} j_1 & j_2 & \cdots & j_k \\ 1\, j_1 & i_2 j_2 & \cdots & i_k j_k \end{pmatrix}$$

heranzieht, die eine Spalte $j_\alpha = i$ enthalten, und wenn man zweitens in den als Koeffizienten auftretenden Polynomen $G^{(j_1, j_2, \ldots, j_k)}_{(1 j_1, i_2 j_2, \ldots, i_k j_k)}$ stets y_i an Stelle von y_1 setzt. Aus der ersten Aussage folgt insbesondere, daß das von den $g^{(j)}_{ik}$ freie Glied bei Δ_i identisch mod. l verschwindet. Die analogen Entwicklungen gelten natürlich für $u_2, u_3, \ldots, u_n$. Setzen wir etwa

$$u_2(y_1, y_2, \ldots, y_n) = \lambda_1 \Delta^{(2)}_1 + \lambda_2 \Delta^{(2)}_2 + \cdots + \lambda_n \Delta^{(2)}_n,$$

wobei $\Delta^{(2)}_i$ jene Determinante ist, die bei Streichung der zweiten Spalte der Matrix entsteht, wenn außerdem von den letzten $\binom{n}{2}$ Spalten nur diejenigen beibehalten werden, die das Element y_i enthalten, so folgt aus den obigen Entwicklungen, daß $\Delta^{(2)}_1$ für $y_1 = 1$ keinen Term $y_2^{l-1} y_3^{l-1} \cdots y_n^{l-1}$ enthält.

Für $y_1 \equiv 1(l)$, $\lambda_1 \equiv 1(l)$, $\lambda_2 \equiv \lambda_3 \equiv \cdots \equiv \lambda_n \equiv 0\,(l)$, gilt daher:

$$\begin{aligned} u_1(1, y_2, \ldots, y_n) &\equiv \pm y_2^{l-1} y_3^{l-1} \cdots y_n^{l-1} + G_{11}(y_2, y_3, \ldots, y_n)\ (l) \\ u_2(1, y_2, \ldots, y_n) &\equiv G_{12}(y_2, y_3, \ldots, y_n)\ (l) \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ u(1, y_2, \ldots, y_n) &\equiv G_{1n}(y_2, y_3, \ldots, y_n)\ (l). \end{aligned}$$

Die $G_{1j}(y_2, y_3 \ldots, y_n)$, $(j = 1, 2, \ldots, n)$, bedeuten dabei Polynome in $y_2, y_3, \ldots, y_n$, die keinen Term $y_2^{l-1} y_3^{l-1} \cdots y_n^{l-1}$ enthalten. Ebenso gilt allgemein:

$$\begin{aligned} u_1(y_1, \ldots, y_{j-1}, 1, y_{j+1}, \ldots, y_n) &\equiv G_{j1}\ (y_1, \ldots, y_{j-1}, y_{j+1}, \ldots, y_n)(l) \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ u_{j-1}(y_1, \ldots, y_{j-1}, 1, y_{j+1}, \ldots, y_n) &\equiv G_{jj-1}(y_1, \ldots, y_{j-1}, y_{j+1}, \ldots, y_n)(l) \\ u_j(y_1, \ldots, y_{j-1}, 1, y_{j+1}, \ldots, y_n) &\equiv \pm y_1^{l-1} \cdots y_{j-1}^{l-1} y_{j+1}^{l-1} \cdots y_n^{l-1} + G_{jj}\ (y_1, \ldots, y_{j-1}, y_{j+1}, \ldots, y_n)(l) \\ u_{j+1}(y_1, \ldots, y_{j-1}, 1, y_{j+1}, \ldots, y_n) &\equiv G_{jj+1}(y_1, \ldots, y_{j-1}, y_{j+1}, \ldots, y_n)(l) \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots, \\ u_n(y_1, \ldots, y_{j-1}, 1, y_{j+1}, \ldots, y_n) &\equiv G_{jn}\ (y_1, \ldots, y_{j-1}, y_{j+1}, \ldots, y_n)(l). \end{aligned}$$

Die Determinante

$$(6) \qquad |u_i(y_1^{(j)}, y_2^{(j)}, \ldots, y_{j-1}^{(j)}, 1, y_{j+1}^{(j)}, \ldots, y_n^{(j)}|$$

enthält daher einen einzigen Term

$$\prod_{j=1}^{n} (y_1^{(j)} y_2^{(j)} \cdots y_{j-1}^{(j)} y_{j+1}^{(j)} \cdots y_n^{(j)})^{l-1}.$$

Sie verschwindet also nicht identisch mod. l. Nach Hilfssatz 4 gibt es folglich n Systeme von Zahlen

$$y_1^{(j)}, y_2^{(j)}, \ldots, y_{j-1}^{(j)}, 1, y_{j+1}^{(j)}, \ldots, y_n^{(j)}, \qquad (j = 1, 2, \ldots, n),$$

so daß (6) einen nicht durch l teilbaren Wert annimmt. In jedem der n Körper $k(y_1^{(j)}, y_2^{(j)}, \ldots, y_{j-1}^{(j)}, 1, y_{j+1}^{(j)}, \ldots, y_n^{(j)})$, $(y = 1, 2, \ldots, n)$, wird dann genau eine Klasse Hauptklasse, derart, daß diese n Klassen eine Basis für das Klassensystem des Grundkörpers bilden. Damit ist der Beweis von Satz II und somit auch von Satz I erbracht.

§ 5.

Es lassen sich zweistufige Gruppen $\mathfrak{G} = S_1^{x_1} S_2^{x_2} \cdots S_n^{x_n} \mathfrak{C}$, $(0 \leqq x_i < l)$, angeben, welche die in Satz I genannte Bedingung nicht erfüllen und trotzdem die Eigenschaft haben, daß für jeden Grundkörper k, welcher die betreffende Gruppe als Relativgruppe des zweiten Klassenkörpers besitzt, der Hauptidealsatz in verschärfter Form gilt. Ob

diese Gruppen aber tatsächlich als Relativgruppen zweiter Klassenkörper auftreten, ist nicht entschieden. Man kann daher noch nicht sagen, ob die in Satz I angeführte Bedingung nur hinreichend oder auch notwendig ist.

Während für $l = 2$ der Hauptidealsatz für jeden Grundkörper in der verschärften Form gilt, ist dies für $l > 2$ nicht immer der Fall. Ein Beispiel dafür liefert die zweistufige Gruppe

$$\mathfrak{G} = S_1^{x_1} S_2^{x_2} T_{12}^{x_3}, \qquad (0 \leqq x_i < 3),$$

mit den Relationen

$$(1) \qquad S_1^{-1} S_2^{-1} S_1 S_2 = T_{12}, \quad S_1^l = T_{12}, \quad S_2^l = E.$$

Aus den Beziehungen

$$S_i^{\Delta_k} = T_{ik}^{1+s_i+\cdots+s_i^{l-1}}, \qquad (i, k = 1, 2, \ldots, l),$$

folgt, daß

$$T_{12}^l = E \quad \text{und} \quad T_{12}^{\Delta_1} = T_{12}^{\Delta_2} = E.$$

Ist k ein Zahlkörper mit der Klassengruppe

$$c_1^{x_1} c_2^{x_2}, \qquad (0 \leqq x_i < l),$$

und ist die Relativgruppe des zweiten Klassenkörpers in bezug auf k von der obigen Struktur, so kann in keinem unverzweigten relativ zyklischen Oberkörper von k vom Relativgrad l eine Klasse $c_1 c_2^{u_2}$, $(0 \leqq u_2 < l)$, in die Hauptklasse übergehen. Dieses gruppentheoretische Gegenbeispiel hat natürlich erst dann Bedeutung für die Theorie der algebraischen Zahlkörper, wenn es einen Grundkörper k gibt, dessen zweiter Klassenkörper die betreffende Relativgruppe in bezug auf den Grundkörper besitzt. Die Kenntnis eines Körpers mit der Klassengruppe $c_1^{x_1} c_2^{x_2}$, $(0 \leqq x_i < 3)$, dessen zweiter Klassenkörper diese Relativgruppe besitzt, verdanke ich einer brieflichen Mitteilung von Herrn A. Scholz:

Unter K_p^l(p, l Primzahlen) werde der Unterkörper l-ten Grades des Körpers der p-ten Einheitswurzeln verstanden. Bekanntlich hat jeder K_p^l eine zu l teilerfremde Klassenzahl. Der Körper $K^9 = K_{19}^3 \cdot K_{1129}^3$ besitzt vier Unterkörper dritten Grades, nämlich K_{19}^3, K_{1129}^3 und zwei weitere Körper, die wir mit $K_{19 \cdot 1129}^3$ und $\bar{K}_{19 \cdot 1129}^3$ bezeichnen wollen. Jeder dieser beiden Körper hat die Eigenschaft, daß sein zweiter Klassenkörper die Gruppe mit den Relationen (1) als Relativgruppe besitzt. Denn K^9 ist unverzweigt über $K_{19 \cdot 1129}^3$, also ist auch der Klassenkörper K von K^9 ein unverzweigter Oberkörper von $K_{19 \cdot 1129}^3$. Die Primzahlen 19 und 1129 sind außerdem so gewählt, daß K die folgende zweistufige Gruppe über $R(1)$ hat:

$$\mathfrak{H} = R_1^{x_1} R_2^{x_2} \mathfrak{C}, \qquad 0 \leqq x_i < 3.$$

Dabei gilt für die Kommutatorgruppe $\mathfrak{C}$:

$$R_1^{-1} R_2^{-1} R_1 R_2 = Q_{12}, \quad Q_{12}^{R_1 - 1} \neq E, \quad Q_{12}^{(R_1-1)^2} = E, \quad Q_{12}^{R_2-1} = E, \quad R_1^3 = R_2^3 = E.$$

$\mathfrak{H}$ enthält die Untergruppe

$$\mathfrak{G} = \{R_1 R_2,\ Q_{12},\ Q_{12}^{R_1-1}\}.$$

Setzen wir

$$R_1 R_2 = S_1, \quad Q_{12} = S_2, \quad Q_{12}^{R_1-1} = T_{12},$$

so erkennen wir, daß $\mathfrak{G}$ die Relationen (1) besitzt. Der Unterkörper $K_{19 \cdot 1129}^3$ von K, der zu $\mathfrak{G}$ gehört, besitzt also einen unverzweigten, relativ zweistufigen Oberkörper, dessen Relativgruppe die Relationen (1) hat. Die Gruppe $\mathfrak{G}$ besitzt notwendig die Relationen

$$T_{12}^l = T_{12}^{\Delta_1} = T_{12}^{\Delta_2} = E.$$

Ihre Kommutatorgruppe ist daher bereits von maximaler Ausdehnung, und das bedeutet, daß K schon der volle zweite Klassenkörper von $k = K_{19 \cdot 1129}^{3}$ ist, wenn K den ersten Klassenkörper von k enthält, und das folgt wieder daraus, daß K selbst der erste Klassenkörper des k enthaltenden, in bezug auf k relativ abelschen Körpers $K_{19}^{3} \cdot K_{1129}^{3}$ ist. — Damit der Klassenkörper von $K_p^3 K_q^3$ die Gruppe $\mathfrak{H}$ in bezug auf $R(1)$ besitzt, ist notwendig und hinreichend, daß die Grundeinheit ε_p des kubischen Körpers K_p^3 kubischer Rest mod. q ist und daß die Grundeinheit ε_q von K_q^3 den gleichen, nichtkubischen Restcharakter für alle drei Primteiler von p hat [1]). Diese Bedingung ist für $p = 19$, $q = 1129$ tatsächlich erfüllt.

Eine Aussage über die Möglichkeit gruppentheoretischer Gegenbeispiele gegen die Verschärfung des Hauptidealsatzes liefert der folgende

Satz III. *Für jede natürliche Zahl n und jede ungerade Primzahl l läßt sich eine zweistufige Gruppe*

$$\mathfrak{G} = S_1^{x_1} S_2^{x_2} \cdots S_n^{x_n} \mathfrak{C}, \qquad (0 \leqq x_i < l),$$

angeben, so daß für jeden Grundkörper, dessen zweiter Klassenkörper die Relativgruppe $\mathfrak{G}$ hat, der Hauptidealsatz nicht in der verschärften Fassung besteht.

Beweis. Wir gelangen zu einer solchen Gruppe, wenn wir die folgenden Stammrelationen annehmen:

$$\begin{aligned} S_1^l &= T_{12} \\ S_2^l &= E \\ &\cdots\cdots \\ S_n^l &= E. \end{aligned}$$

Weiter werde über die Gruppe vorausgesetzt, daß sie das folgende „vollständige System“ von Relationen besitze:

$$\begin{aligned} T_{ik}^{\Delta j} T_{kj}^{\Delta i} T_{ji}^{\Delta k} &= E, \\ S_i^{l\Delta_k} &= T_{ik}^{1+s_i+\cdots+s_i^{l-1}}, \\ T_{ki}^{l} &= E, \\ T_{ik}^{\Delta_{i_1}\Delta_{i_2}\cdots\Delta_{i_{l-1}}} &= E. \end{aligned}$$

Ist $c_1^{x_1} c_2^{x_2} \cdots c_n^{x_n}$, $(0 \leqq x_i < l)$, die Klassengruppe von k, so entspricht c_1 im Körper $k(y)$ die Substitution

$$T_{12}^{1+\Delta_2^{l-2} y_{11}} T_{13}^{\Delta_3^{l-2} y_{12}} \cdots T_{1n}^{\Delta_n^{l-2} y_{12\ldots n-1}},$$

und es könnte eine Klasse $c_1 c_2^{u_2} \cdots c_n^{u_n}$ nur in einem solchen Körper $k(y_1, y_2, \ldots, y_n)$ Hauptklasse werden, für den $y_1 \equiv y_2 \equiv 0\ (l)$ ist. Wir betrachten einen solchen durch

$$y_3 x_3 + \cdots + y_n x_n \equiv 0\ (l)$$

bestimmten Oberkörper und wählen die Numerierung so, daß $y_3 \not\equiv 0 (l)$ sei. In diesem Körper entspricht der Klasse c_1 die Substitution $T_{13}^{\Delta_3^{l-2}}$, der Klasse c_2 die Substitution $T_{23}^{\Delta_3^{l-2}}$, jeder Klasse c_i, $i > 2$, das Element $T_{i3}^{\Delta_3^{l-2}}$. Da kein Element $\prod_{\substack{i \neq 3 \\ 0<u_i<l}} T_{i3}^{\Delta_3^{l-2} u_i}$ in der zugehörigen Gruppe $\mathfrak{C}(y)$ liegt, kann also keine Klasse $c_1 c_2^{u_2} \cdots c_n^{u_n}$ in $k(y)$ in der Hauptklasse liegen, womit Satz III bewiesen ist.

---

[1]) Siehe A. Scholz, Heidelberger Akademie-Berichte 1930, Über das Verhältnis von Idealklassen- und Einheitengruppe in Abelschen Körpern von Primzahlpotenzgrad.

Eingegangen 23. November 1931.

Zur Transzendenz von e^{π} *).

Von *J. F. Koksma* in Hilversum (Niederlande) und *J. Popken* in Smilde (Niederlande).

Bekanntlich hat Herr A. Gelfond [1]) bewiesen, daß die Zahl e^{π} transzendent ist. Wie wir in dieser Abhandlung zeigen, reicht die Gelfondsche Methode nicht nur aus die Transzendenz von e^{π} zu beweisen, sondern sie liefert auch ein Resultat über das Transzendenzmaß dieser Zahl. Wir beweisen nämlich folgenden

Satz. *Bezeichnet ε eine positive Zahl,*

$$\mathrm{B}(x) = b_0 + b_1 x + \cdots + b_g x^g \tag{1}$$

ein Polynom mit ganzen rationalen Koeffizienten, das nicht identisch verschwindet, und ist

$$B = \max_{\gamma=0,1,\ldots,g} (|b_\gamma|, 3), \tag{2}$$

so gibt es eine nur von g und ε abhängige positive Zahl C, derart daß

$$|\mathrm{B}(e^{\pi})| > CB^{-(4+\varepsilon)\frac{\log B}{\log\log B}} \tag{3}$$

ist.

Bemerkung 1. Wir werden sogar einen allgemeineren Satz beweisen, der den vorigen als Spezialfall enthält. Wir zeigen nämlich, daß dieser Satz bestehen bleibt, wenn $\mathrm{B}(x)$ ein nicht identisch verschwindendes Polynom ist mit Koeffizienten b_γ, die ganze Zahlen im Gaußschen Körper $\mathrm{K}(i)$ sind, während B wieder durch (2) definiert ist.

Bemerkung 2. Es sei θ eine beliebige algebraische Zahl, die der irreduziblen Gleichung mit ganzen rationalen Koeffizienten

$$\mathrm{B}(x) = b_0 + b_1 x + \cdots + b_g x^g = 0, \qquad (b_0, b_1, \ldots, b_g) = 1\ ^{2})$$

genügt; die durch (2) dargestellte Zahl B heiße die Höhe von θ [3]). Wir zeigen am Schluß der Abhandlung, daß man den Satz auf die folgende Gestalt bringen kann:

Ist ε eine positive Zahl, θ eine algebraische Zahl vom Grade g und von der Höhe B, so gibt es eine nur von g und ε abhängige positive Zahl $\bar{C}$, derart daß

$$|e^{\pi} - \theta| > \bar{C} e^{-(4+\varepsilon)\frac{\log B}{\log\log B}} \tag{4}$$

ist.

Bemerkung 3. In einer älteren (nicht publizierten) Fassung dieser Abhandlung fanden wir ein schwächeres Ergebnis. Statt (3) wurde gefunden

$$|\mathrm{B}(e^{\pi})| > CB^{-u\frac{\log B}{\log\log B}}, \tag{5}$$

---

*) Die Anregung zu dieser Arbeit verdanken wir Herrn E. Landau, dem wir an dieser Stelle herzlich Dank sagen.

[1]) A. Gelfond, C. R. **189** (1929), S. 1224.

[2]) Mit $(b_0, b_1, \ldots, b_g)$ wird der größte gemeinsame Teiler von $b_0, b_1, \ldots, b_g$ gemeint.

[3]) Vgl. C. Siegel, Approximation algebraischer Zahlen, Math. Zeitschrift **10** (1921), S. 178.

wo u und C nicht näher angegebene nur von g abhängige positive Zahlen bedeuten. Herr C. L. Siegel teilte uns brieflich eine andere Methode als die unsrige mit, um aus den Hilfssätzen 8 und 9 den Satz herzuleiten. Diese Methode gestattete, die Zahl u (und zwar unabhängig von g) zu bestimmen. Mit freundlicher Genehmigung von Herrn Siegel haben wir in der letzten Hälfte der Abhandlung von seiner Methode Gebrauch gemacht. Bei der Durchführung wurde in (5) dann $u = 4 + \varepsilon$ gefunden.

Bemerkung 4. Die Methode unserer Arbeit ist allgemeiner auch anwendbar, wenn man statt $e^{\pi} = (-1)^{-i}$ eine Zahl der Gestalt a^{α} betrachtet, wo a ganz-algebraisch $\neq 0$ und $\neq 1$ ist, und α eine quadratische Irrationalzahl ist.

Wir schicken dem Beweise des Satzes 13 Hilfssätze voran. In der Folge seien $\zeta_0, \zeta_1, \zeta_2, \ldots$ die ganzen Zahlen des Gaußschen Körpers. Diese Zahlen seien nach steigender Norm und, bei demselben Absolutbetrag, nach steigendem Argument angeordnet; also $\zeta_0 = 0$, $\zeta_1 = 1$, $\zeta_2 = i$ usw.

Weiter setzen wir für $n \geqq 0$

$$F_n(z) = \prod_{\nu=0}^{n} (z - \zeta_\nu) \tag{6}$$

und überdies

$$\begin{cases} \varphi(0, 0) = 1, \\ \varphi(n, \nu) = F_n'(\zeta_\nu) = \prod\limits_{\substack{\mu=0 \\ \mu \neq \nu}}^{n} (\zeta_\nu - \zeta_\mu) \qquad (n \geqq 1;\ \nu = 0, 1, \ldots, n). \end{cases} \tag{7}$$

Hilfssatz 1. *Seien K_1 und K_2 zwei Kreise in der Gaußschen Ebene vom gleichen Radius $r \geqq \frac{1}{2}$. Bezeichnet A_1 die Anzahl der Gitterpunkte in K_1 und A_2 die Anzahl der Gitterpunkte in K_2, wobei man Gitterpunkte auf dem Rande nach Belieben mitrechnen oder weglassen kann, dann ist*

$$|A_1 - A_2| < 19r \tag{8}$$

und für $r \geqq \frac{3}{2}$

$$\pi(r - \tfrac{3}{2})^2 \leqq A_\sigma \leqq \pi(r + \tfrac{3}{2})^2 \qquad (\sigma = 1, 2). \tag{9}$$

Beweis. Wir unterscheiden zwei verschiedene Fälle.

1. Es sei $\frac{1}{2} \leqq r < \frac{3}{2}$. Jeden der Kreise K_1 und K_2 umschließen wir mit einem den Koordinatenachsen parallel gerichteten Quadrat von der Kantenlänge 3, das den betreffenden Kreis ganz in seinem Innern enthält. Weil es im Innern jedes der beiden Quadrate höchstens 9 Gitterpunkte gibt, gilt folglich

$$A_1 \leqq 9, \quad A_2 \leqq 9, \quad \text{also} \quad |A_1 - A_2| \leqq 9 < 19r.$$

2. Es sei $r \geqq \frac{3}{2}$. Man kann wegen $\sqrt{2} < \frac{3}{2}$ um den Mittelpunkt jedes der beiden Kreise K_1 und K_2 zwei Kreise zeichnen mit den Radien

$$r + \sqrt{2} \quad \text{und} \quad r - \sqrt{2};$$

in dieser Weise finden wir nach bekannten Überlegungen, wobei jedem Gitterpunkt ein Quadrat zugeordnet wird,

$$\pi(r - \tfrac{3}{2})^2 \leqq \pi(r - \sqrt{2})^2 \leqq A_\sigma \leqq \pi(r + \sqrt{2})^2 \leqq \pi(r + \tfrac{3}{2})^2 \qquad (\sigma = 1, 2),$$

womit (9) bewiesen ist. Außerdem folgt hieraus

$$|A_1 - A_2| \leqq \pi(r + \tfrac{3}{2})^2 - \pi(r - \tfrac{3}{2})^2 = 6\pi r < 19r.$$

Hiermit ist Hilfssatz 1 bewiesen.

Hilfssatz 2 [4]). *Es gibt ein $c_1 < 1$, so daß*

---

[4]) Die Zahlen $c_1, c_2, \ldots, c_{18}$ bezeichnen in der Folge stets positive absolute Konstanten.

(10) $$c_1\sqrt{n} \leqq |\zeta_n| \leqq \sqrt{n} \qquad (n \geqq 0)$$

ist.

Beweis. Wir unterscheiden zwei verschiedene Fälle.

1. Es sei $0 \leqq n \leqq 14$. Dann ist

$$\begin{aligned} |\zeta_0| &= 0 \leqq \sqrt{0}, \\ |\zeta_1| = |\zeta_2| = |\zeta_3| = |\zeta_4| &= 1 \leqq \sqrt{1}, \\ |\zeta_5| = |\zeta_6| = |\zeta_7| = |\zeta_8| &= \sqrt{2} \leqq \sqrt{5}, \\ |\zeta_9| = |\zeta_{10}| = |\zeta_{11}| = |\zeta_{12}| &= 2 \leqq \sqrt{9}, \\ |\zeta_{13}| = |\zeta_{14}| &= \sqrt{5} \leqq \sqrt{13}. \end{aligned}$$

2. Es sei $n > 14$ und K ein Kreis mit Mittelpunkt 0 und Radius $|\zeta_n|$. Nach Definition von ζ_n liegen im Inneren und auf einem gewissen Teil dieses Kreises n Gitterpunkte. Wir können deshalb Formel (9) von Hilfssatz 1 anwenden mit

$$\sigma = 1, \quad K_1 = K, \quad r = |\zeta_n| \geqq \sqrt{5} > \tfrac{3}{2}, \quad A_r = n;$$

folglich

$$\pi(|\zeta_n| - \tfrac{3}{2})^2 \leqq n \leqq \pi(|\zeta_n| + \tfrac{3}{2})^2,$$

also

$$\sqrt{\frac{n}{\pi}} - \frac{3}{2} \leqq |\zeta_n| \leqq \sqrt{\frac{n}{\pi}} + \frac{3}{2};$$

bei geeignetem $c_2 < 1$ gilt folglich wegen $\sqrt{\pi} > 1{,}7$ und $n \geqq 15$

$$c_2\sqrt{n} \leqq |\zeta_n| \leqq \frac{\sqrt{n}}{1{,}7} + \frac{3}{2\sqrt{15}}\sqrt{n} < \sqrt{n}\left(\frac{3}{5} + \frac{3}{2}\frac{4}{15}\right) = \sqrt{n}.$$

Mit Rücksicht auf Fall 1 folgt hieraus bei geeignetem $c_1 \leqq c_2$ die Ungleichung (10), so daß Hilfssatz 2 hiermit bewiesen ist.

Hilfssatz 3. *Es ist für* $n \geqq 1$

(11) $$e^{\frac{1}{2}n\log n - c_3 n} \leqq |\varphi(n, 0)| \leqq e^{\frac{1}{2}n\log n},$$

wo $\varphi(n, 0)$ *durch* (7) *definiert ist.*

Beweis. Aus (7) folgt wegen $\zeta_0 = 0$

$$|\varphi(n, 0)| = \prod_{\mu=1}^{n} |\zeta_\mu|.$$

Nach (10) ist also

$$c_1^n\sqrt{n!} \leqq |\varphi(n, 0)| \leqq (\sqrt{n})^n.$$

Bekanntlich ist aber

$$n! \geqq n^n e^{-n},$$

folglich gilt

$$e^{\frac{1}{2}n\log n - \frac{n}{2} + n\log c_1} \leqq |\varphi(n, 0)| \leqq e^{\frac{1}{2}n\log n},$$

so daß Hilfssatz 3 mit

$$c_3 = \tfrac{1}{2} - \log c_1$$

bewiesen ist (man beachte $c_1 < 1$).

Hilfssatz 4. *Es sei* $\gamma \neq 0$ *irgendeine ganze Zahl aus* $\mathsf{K}(i)$, $g(n, \nu, \gamma)$ für $0 \leqq \nu \leqq n$ $(n \geqq 1)$ *die Anzahl der durch* γ *teilbaren Zahlen unter den* n *Faktoren* $\zeta_\nu - \zeta_\mu$ *in* $\varphi(n, \nu)$. *Dann ist*

(12) $$g(n, \nu, \gamma) = 0 \quad \textit{für} \quad |\gamma| > 2|\zeta_n|$$

und

$$|g(n, \nu, \gamma) - g(n, 0, \gamma)| \leqq 19 \frac{|\zeta_n|}{|\gamma|}. \tag{13}$$

Beweis. *Zu* (12). Aus der Definition von ζ_ν folgt

$$|\zeta_\nu - \zeta_\mu| \leqq 2\,|\zeta_n| < |\gamma| \qquad (0 \leqq \nu \leqq n;\ 0 \leqq \mu \leqq n).$$

Hieraus folgt sogleich (12).

Zu (13). Ohne Beschränkung der Allgemeinheit können wir setzen

$$|\gamma| \leqq 2\,|\zeta_n|; \tag{14}$$

andernfalls ist (13) eine triviale Folge von (12). Wegen der Definition von $g(n, \nu, \gamma)$ und $\varphi(n, \nu)$ ist die Anzahl der ζ_μ mit der Eigenschaft

$$\zeta_\nu - \zeta_\mu \equiv 0 \pmod{\gamma} \qquad (0 \leqq \mu \leqq n) \tag{15}$$

für jedes feste ν $(0 \leqq \nu \leqq n)$ gleich $1 + g(n, \nu, \gamma)$.

Aus (15) folgt, daß es eine ganze Zahl ξ in $\mathsf{K}(i)$ gibt mit

$$\zeta_\nu - \zeta_\mu = \xi\gamma,$$

also

$$|\xi\gamma - \zeta_\nu| = |\zeta_\mu| \leqq |\zeta_n|,$$

oder

$$\left|\xi - \frac{\zeta_\nu}{\gamma}\right| \leqq \frac{|\zeta_n|}{|\gamma|}. \tag{16}$$

Jede Lösung ζ_μ von (15) gibt also einen Gitterpunkt ξ innerhalb oder auf dem Rande des Kreises, der durch (16) dargestellt wird, wenn ξ als Variable betrachtet wird. Umgekehrt gibt jede Lösung ξ von (16) mit Ausnahme einer gewissen Anzahl auf dem Rande eine Lösung

$$\zeta_\mu = \zeta_\nu - \xi\gamma$$

von (15).

Hieraus folgt, daß die Anzahl $1 + g(n, \nu, \gamma)$ der Lösungen ζ_μ von (15) gleich der Anzahl der Gitterpunkte ist, die innerhalb oder auf einem gewissen Teil des Randes von (16) liegen.

Wir wenden jetzt Hilfssatz 1 an und verstehen dabei unter K_1 den Kreis (16) mit $\nu = 0$ und unter K_2 den Kreis (16) mit beliebigem $\nu (0 \leqq \nu \leqq n)$. Dann ist $r = \frac{|\zeta_n|}{|\gamma|} \geqq \frac{1}{2}$, wegen (14).

Hilfssatz 1 lehrt uns also

$$|A_1 - A_2| = |g(n, 0, \gamma) - g(n, \nu, \gamma)| < 19r = 19\frac{|\zeta_n|}{|\gamma|},$$

womit (13) und damit Hilfssatz 4 vollständig bewiesen ist.

Hilfssatz 5. *Für $u \geqq 2$ ist die über alle (gewöhnlichen) Primzahlen $p \leqq u$ erstreckte Summe*

$$\sum_{p \leqq u} \frac{\log p}{\sqrt{p}} < c_4 \sqrt{u}. \tag{17}$$

Beweis. Bekanntlich [5]) ist für $h > 1$, wenn p_h die h-te Primzahl bezeichnet,

$$c_5 h \log h < p_h < c_6 h \log h,$$

also

$$\frac{\log p_h}{\sqrt{p_h}} < \frac{\log (c_6 h \log h)}{\sqrt{c_5 h \log h}} = \frac{\log c_6 + \log h + \log\log h}{\sqrt{c_5}\sqrt{h}\sqrt{\log h}} < c_7 \sqrt{\frac{\log h}{h}},$$

mit geeignetem c_7, das wir $> \frac{1}{\sqrt{2}}$ wählen können.

[5]) Vgl. etwa E. Landau, Vorlesungen über Zahlentheorie I, Satz 113, S. 68.

Bezeichne $\pi(u)$ die Anzahl der Primzahlen $\leqq u$, dann ist also

$$\sum_{p\leqq u}\frac{\log p}{\sqrt{p}}=\sum_{h=1}^{\pi(u)}\frac{\log p_h}{\sqrt{p_h}}<\frac{\log 2}{\sqrt{2}}+c_7\sum_{h=2}^{\pi(u)}\sqrt{\frac{\log h}{h}}<c_7\sqrt{\log u}\sum_{h=1}^{\pi(u)}\frac{1}{\sqrt{h}},$$

wegen $\dfrac{\log 2}{\sqrt{2}}<c_7\sqrt{\log 2}\leqq c_7\sqrt{\log u}$; hierin ist bekanntlich [6])

$$\pi(u)<c_8\frac{u}{\log u}.$$

Man hat also

$$\sum_{p\leqq u}\frac{\log p}{\sqrt{p}}<c_7\sqrt{\log u}\sum_{h=1}^{\left[c_8\frac{u}{\log u}\right]}\frac{1}{\sqrt{h}}\ [7])$$

$$<c_7\sqrt{\log u}\left(1+\int_1^{\left[c_8\frac{u}{\log u}\right]}\frac{dx}{\sqrt{x}}\right)$$

$$<2c_7\sqrt{\log u}\sqrt{c_8\frac{u}{\log u}}=c_4\sqrt{u}.$$

Hiermit ist Hilfssatz 5 mit $c_4=2c_7\sqrt{c_8}$ bewiesen.

Hilfssatz 6. *Wir bezeichnen mit ϱ eine Primzahl im Gaußschen Körper $\mathsf{K}(i)$ mit*

$$R(\varrho)>0,\quad J(\varrho)\geqq 0\ [8]).$$

Für $n\geqq 1$ sei

$$\omega(n)=\prod_{|\varrho|\leqq 2|\zeta_n|}\varrho^{\left[19\frac{|\zeta_n|}{|\varrho|-1}\right]},\tag{18}$$

und für $0\leqq\nu\leqq n(n\geqq 1)$ sei

$$\chi(n,\nu)=\frac{\varphi(n,0)}{\varphi(n,\nu)}\,\omega(n)\tag{19}$$

gesetzt, wo $\varphi(n,\nu)$ durch (7) definiert ist. Unter diesen Voraussetzungen gilt

$$\chi(n,\nu)\ \text{ist ganz in}\ \mathsf{K}(i)\qquad(\nu=0,\ldots,n),\tag{20}$$

$$\chi(n,\nu)\,/\,\omega^2(n)\ [8a])\qquad(\nu=0,\ldots,n)\tag{21}$$

und

$$|\omega(n)|<e^{c_9 n}\qquad(n\geqq 1).\tag{22}$$

Beweis. Zu (20). Wegen der Definition von $\varphi(n,\nu)$ in (7) und der Definition von $g(n,\nu,\gamma)$ in Hilfssatz 4 gilt für $\nu=0,1,\ldots,n$

$$\varphi(n,\nu)=\varepsilon(n,\nu)\prod_{|\varrho|\leqq 2|\zeta_n|}\varrho^{\sum_{w=1}^{\infty}g(n,\nu,\varrho^w)},\tag{23}$$

wo $\varepsilon(n,\nu)$ eine geeignet gewählte Einheit des Körpers $\mathsf{K}(i)$ ist. Wir beachten noch, daß nach (12) von Hilfssatz 4 die Reihe $\sum_{w=1}^{\infty}$ im rechten Glied von (23) nach endlich vielen Summanden abbricht.

Setzen wir

$$l(n,\nu,\varrho)=\sum_{w=1}^{\infty}(g(n,\nu,\varrho^w)-g(n,0,\varrho^w)),\tag{24}$$

---

[6]) Vgl. etwa E. Landau, loc. cit., Satz 112, S. 66.

[7]) Für reelles a bezeichnet $[a]$ die größte ganze Zahl $\leqq a$.

[8]) Mit $R(\varrho)$ bezeichnen wir den Realteil, mit $J(\varrho)$ den Imaginärteil von ϱ.

[8a]) a/b bedeutet „a teilt b“; $a\nmid b$ „a teilt b nicht“.

so folgt aus (23)

$$\frac{\varphi(n,0)}{\varphi(n,\nu)} = \frac{\varepsilon(n,0)}{\varepsilon(n,\nu)} \prod_{|\varrho|\leqq 2|\zeta_n|} \varrho^{-l(n,\nu,\varrho)}.$$

Deshalb folgt aus (19) und (18)

$$\chi(n,\nu) = \frac{\varepsilon(n,0)}{\varepsilon(n,\nu)} \prod_{|\varrho|\leqq 2|\zeta_n|} \varrho^{-l(n,\nu,\varrho)+\left[19\frac{|\zeta_n|}{|\varrho|-1}\right]}. \tag{25}$$

Durch Anwendung von Hilfssatz 4 finden wir aus (13) und (24)

$$|l(n,\nu,\varrho)| \leqq 19\,|\zeta_n| \sum_{w=1}^{\infty} \frac{1}{|\varrho|^w} = 19\,\frac{|\zeta_n|}{|\varrho|-1}. \tag{26}$$

Da wegen (24) für $0 \leqq \nu \leqq n$ die Zahl $l(n,\nu,\varrho)$ ganz rational ist, geht aus (25) und (26) hervor, daß $\chi(n,\nu)$ eine ganze Zahl in $K(i)$ ist.

Zu (21). Aus (25) und (18) folgt

$$\frac{\omega^2(n)}{\chi(n,\nu)} = \frac{\varepsilon(n,\nu)}{\varepsilon(n,0)} \prod_{|\varrho|\leqq 2|\zeta_n|} \varrho^{l(n,\nu,\varrho)+\left[19\frac{|\zeta_n|}{|\varrho|-1}\right]}; \tag{27}$$

mit Rücksicht auf (26) schließen wir also, daß die rechte Seite von (27) eine ganze Zahl in $K(i)$ ist, also daß (21) gilt.

Zu (22). Aus (18) geht

$$|\omega(n)| \leqq \prod_{|\varrho|\leqq 2|\zeta_n|} |\varrho|^{19\frac{|\zeta_n|}{|\varrho|-1}}$$

hervor; nach Hilfssatz 2 gilt also

$$|\omega(n)| \leqq e^{19\sqrt{n}\sum\limits_{|\varrho|\leqq 2\sqrt{n}} \frac{\log|\varrho|}{|\varrho|-1}} \leqq e^{c_{10}\sqrt{n}\sum\limits_{|\varrho|\leqq 2\sqrt{n}} \frac{\log|\varrho|}{|\varrho|}}. \tag{28}$$

Bekanntlich[9]) besteht zwischen unseren Körperprimzahlen $\varrho(R(\varrho)>0,\ J(\varrho)\geqq 0)$ und den gewöhnlichen Primzahlen p eine Korrespondenz, so daß jedem ϱ nur eine Primzahl p und jedem p höchstens zwei Zahlen ϱ entsprechen, und zwar gilt dabei für je zwei korrespondierende Zahlen ϱ und p

$$\sqrt{p} \leqq |\varrho| \leqq p.$$

Aus (28) folgt also

$$|\omega(n)| < e^{c_{11}\sqrt{n}\sum\limits_{p\leqq 4n} \frac{\log p}{\sqrt{p}}}.$$

Wir wenden jetzt Hilfssatz 5 an mit $u = 4n$; wegen $n \geqq 1$ ist $u \geqq 4$. Formel (17) lehrt uns dann

$$|\omega(n)| < e^{c_{11}\sqrt{n}\cdot c_4\sqrt{4n}} = e^{c_9 n},$$

womit Hilfssatz 6 vollständig bewiesen ist.

Hilfssatz 7[9a]). *Wird $F_n(z)$ für $n \geqq 0$ durch* (6) *definiert, und wird außerdem*

$$F_{-1}(z) = 1 \tag{29}$$

gesetzt, so gilt für $s \geqq 0$ und für beliebige z und x $(x \neq z,\ x \neq \zeta_\nu (\nu = 0, 1, \ldots, n))$

$$\sum_{\sigma=0}^{s} \frac{F_{\sigma-1}(z)}{F_\sigma(x)} = \frac{1}{x-z}\left\{1 - \frac{F_s(z)}{F_s(x)}\right\}. \tag{30}$$

Beweis. Für $\sigma \geqq 0$ ist

$$\frac{1}{x-z} = \frac{1}{x-\zeta_\sigma} + \frac{z-\zeta_\sigma}{x-\zeta_\sigma}\cdot\frac{1}{x-z},$$

---

[9]) Vgl. etwa E. Landau, loc. cit. III, Satz 598, S. 12.

[9a]) Dieser Hilfssatz ist bekannt aus der Theorie der Newtonschen Interpolationsreihe, ebenso wie gewisse Teile des Beweises des folgenden Hilfssatzes.

also wegen (6) und (29)

$$\frac{F_{\sigma-1}(z)}{F_{\sigma-1}(x)}\cdot\frac{1}{x-z}=\frac{F_{\sigma-1}(z)}{(x-\zeta_\sigma)F_{\sigma-1}(x)}+\frac{(z-\zeta_\sigma)F_{\sigma-1}(z)}{(x-\zeta_\sigma)F_{\sigma-1}(x)}\cdot\frac{1}{x-z}=\frac{F_{\sigma-1}(z)}{F_\sigma(x)}+\frac{F_\sigma(z)}{F_\sigma(x)}\cdot\frac{1}{x-z},$$

also

$$\sum_{\sigma=0}^{s}\frac{F_{\sigma-1}(z)}{F_\sigma(x)}=\frac{1}{x-z}\sum_{\sigma=0}^{s}\left\{\frac{F_{\sigma-1}(z)}{F_{\sigma-1}(x)}-\frac{F_\sigma(z)}{F_\sigma(x)}\right\}$$
$$=\frac{1}{x-z}\left\{\frac{F_{-1}(z)}{F_{-1}(x)}-\frac{F_s(z)}{F_s(x)}\right\}=\frac{1}{x-z}\left\{1-\frac{F_s(z)}{F_s(x)}\right\},$$

wegen (29); hiermit ist Hilfssatz 7 bewiesen.

Hilfssatz 8. *Wird für* $n\geqq 0$

$$A_n=\sum_{\nu=0}^{n}\frac{e^{\pi\zeta_\nu}}{\varphi(n,\nu)} \tag{31}$$

gesetzt, so gelten folgende Behauptungen:

Für $n\geqq 4$ *ist*

$$|A_n|<e^{-n\log n+(\pi+1)n}. \tag{32}$$

Für jede Zahl $\lambda(1<\lambda\leqq 2)$ *gibt es eine nur von* λ *abhängige positive Zahl* $c_1'>4$, *so daß für jede natürliche Zahl* $h\geqq c_1'$ *im Intervall*

$$h\leqq n\leqq \lambda h \tag{33}$$

mindestens ein n *liegt mit*

$$|A_n|>e^{-\frac{3\lambda-1}{2\lambda}n\log n}. \tag{34}$$

Beweis. Wir bezeichnen mit K_n einen Kreis mit Mittelpunkt 0 und mit dem Radius

$$r=\operatorname{Max}(n,4). \tag{35}$$

Dann gilt für $0\leqq n<4$

$$|\zeta_n|<r, \tag{36}$$

und für $n\geqq 4$, wegen (10),

$$r=n\geqq 2\sqrt{n}\geqq 2|\zeta_n|>|\zeta_n|;$$

also gilt (36) allgemein für $n\geqq 0$.

Alle Pole der Funktion

$$\frac{e^{\pi x}}{F_n(x)} \qquad (n\geqq 0)$$

liegen deshalb wegen (6) im Innern des Kreises K_n. Wegen (6) und (7) hat man nach dem Residuensatz also

$$\frac{1}{2\pi i}\int_{K_n}\frac{e^{\pi x}}{F_n(x)}\,dx=\sum_{\nu=0}^{n}\frac{e^{\pi\zeta_\nu}}{F_n'(\zeta_\nu)}=\sum_{\nu=0}^{n}\frac{e^{\pi\zeta_\nu}}{\varphi(n,\nu)}.$$

Man hat also nach (31)

$$A_n=\frac{1}{2\pi i}\int_{K_n}\frac{e^{\pi x}}{F_n(x)}\,dx \qquad (n\geqq 0). \tag{37}$$

Zu (32). Jetzt ist $r=n\geqq 4$. Aus (37) folgt wegen (6)

$$|A_n|=\left|\frac{1}{2\pi i}\int_{K_n}\frac{e^{\pi x}}{F_n(x)}\,dx\right|\leqq\frac{1}{2\pi}\int_{K_n}\left|\frac{e^{\pi x}}{F_n(x)}\,dx\right|\leqq\frac{1}{2\pi}\cdot 2\pi n\,\frac{e^{n\pi}}{n\operatorname*{Min}_{|x|=n}\prod_{\nu=1}^{n}|x-\zeta_\nu|}. \tag{38}$$

Wir beachten, daß wegen (10) und $n\geqq 4$ gilt

$$\operatorname*{Min}_{|x|=n}\prod_{\nu=1}^{n}|x-\zeta_\nu| \geqq (n-|\zeta_n|)^n \geqq (n-\sqrt{n})^n \geqq \left(\frac{n}{2}\right)^n.$$

Aus (38) geht also hervor

$$|A_n| \leqq e^{\pi n}\cdot\left(\frac{2}{n}\right)^n < e^{-n\log n+(\pi+1)n},$$

wegen $2<e$, womit (32) bewiesen ist.

Zu (34). Aus (37) folgt für jede ganze rationale Zahl $s \geqq 0$, mit Rücksicht auf $\int_{K_n} = \int_{K_s}$ für $s \geqq n$,

$$\sum_{n=0}^{s} A_n F_{n-1}(z) = \frac{1}{2\pi i}\sum_{n=0}^{s}\int_{K_n} e^{\pi x}\frac{F_{n-1}(z)}{F_n(x)}\,dx = \frac{1}{2\pi i}\int_{K_s}\left(e^{\pi x}\sum_{n=0}^{s}\frac{F_{n-1}(z)}{F_n(x)}\right)dx.$$

Nach Hilfssatz 7 mit n statt σ haben wir also

$$\begin{aligned}\sum_{n=0}^{s} A_n F_{n-1}(z) &= \frac{1}{2\pi i}\int_{K_s}\frac{e^{\pi x}}{x-z}\left(1-\frac{F_s(z)}{F_s(x)}\right)dx\\ &= \frac{1}{2\pi i}\int_{K_s}\frac{e^{\pi x}}{x-z}\,dx - \frac{1}{2\pi i}\int_{K_s} e^{\pi x}\frac{F_s(z)}{(x-z)F_s(x)}\,dx.\end{aligned}$$

Nach dem Residuensatz ist für $|z|<\operatorname{Max}(s,4)$ das erste Integral gleich $e^{\pi z}$. Wir haben also für $s\geqq 0$ und $|z|<\operatorname{Max}(s,4)$

$$e^{\pi z} - \sum_{n=0}^{s} A_n F_{n-1}(z) = \frac{F_s(z)}{2\pi i}\int_{K_s}\frac{e^{\pi x}}{(x-z)F_s(x)}\,dx \quad [10]). \tag{39}$$

Es sei jetzt h eine natürliche Zahl mit

$$h\geqq 4, \quad \text{also} \quad [\lambda h]\geqq 4,$$

wenn λ eine beliebige Zahl mit $1<\lambda\leqq 2$ ist. Aus (39) mit $s=[\lambda h]$ folgt durch h-malige Differentiation nach z (man beachte dabei, daß $F_{n-1}(z)$ ein Polynom vom Grade n ist)

$$\begin{aligned}\pi^h e^{\pi z} - \sum_{n=h}^{[\lambda h]} A_n F_{n-1}^{(h)}(z) &= \sum_{m=0}^{h}\binom{h}{m}\frac{F_{[\lambda h]}^{(m)}(z)}{2\pi i}\frac{d^{h-m}}{dz^{h-m}}\int_{K_{[\lambda h]}}\frac{e^{\pi x}}{(x-z)F_{[\lambda h]}(x)}\,dx\\ &= \sum_{m=0}^{h}\frac{h!}{m!(h-m)!}\frac{F_{[\lambda h]}^{(m)}(z)}{2\pi i}\int_{K_{[\lambda h]}}\frac{(h-m)!\,e^{\pi x}}{(x-z)^{h-m+1}F_{[\lambda h]}(x)}\,dx,\end{aligned}$$

für $|z|<4$; also ist für $z=0$ und $h\geqq 4$

$$\left|\pi^h - \sum_{n=h}^{[\lambda h]} A_n F_{n-1}^{(h)}(0)\right| \leqq \sum_{m=0}^{h}\frac{h!\,|F_{[\lambda h]}^{(m)}(0)|}{m!}\left|\frac{1}{2\pi i}\int_{K_{[\lambda h]}}\frac{e^{\pi x}}{x^{h-m+1}F_{[\lambda h]}(x)}\,dx\right|. \tag{40}$$

Nach Definition von $F_n(z)$ ist

$$\begin{cases} |F_n^{(m)}(0)| \leqq \dfrac{(n+1)!}{(n-m+1)!}\,|\zeta_n|^{n-m+1} & \\ \qquad\leqq \dfrac{(n+1)!}{(n-m+1)!}\,(\sqrt{n})^{n-m+1} & (m\leqq n+1)\end{cases} \tag{41}$$

(der letzte Schritt wegen (10)).

Für $n=[\lambda h]$ und $m\leqq[\lambda h]$ folgt hieraus

$$|F_{[\lambda h]}^{(m)}(0)| \leqq \frac{([\lambda h]+1)!}{([\lambda h]-m+1)!}\,(\lambda h)^{\frac{\lambda h-m+1}{2}},$$

---

[10]) Durch Abschätzung des Restgliedes kann man sogar beweisen, daß $e^{\pi z}=\sum_{n=0}^{\infty}A_n F_{n-1}(z)$ ist, was die bekannte Entwicklung der Funktion $e^{\pi z}$ nach der Newtonschen Interpolationsreihe ist.

also wegen $\lambda \leqq 2$

$$|F^{(m)}_{[\lambda h]}(0)| \leqq \frac{([\lambda h]+1)!}{([\lambda h]-m+1)!}\, e^{c_{12}h}\, h^{\frac{1}{2}\lambda h-\frac{1}{2}m}. \tag{42}$$

Nach Definition von $F_n(z)$ ist weiter für $|x| = [\lambda h]$ mit Rücksicht auf (10)

$$|F_{[\lambda h]}(x)| = [\lambda h]\prod_{\nu=1}^{[\lambda h]} |x-\zeta_\nu| \geqq [\lambda h]([\lambda h]-\sqrt{[\lambda h]})^{[\lambda h]},$$

also wegen $[\lambda h] \geqq 4$ und $1 < \lambda \leqq 2$

$$|F_{[\lambda h]}(x)| \geqq [\lambda h]\left(\frac{[\lambda h]}{2}\right)^{[\lambda h]} > \frac{h\,h^{[\lambda h]}}{2^{\lambda h}} > h^{\lambda h}\, e^{-2h}. \tag{43}$$

Nach der Definition im Anfang dieses Beweises hat $K_{[\lambda h]}$ wegen $\lambda h > h \geqq 4$ den Radius $[\lambda h]$. Aus (43) folgt deshalb für $0 \leqq m \leqq h$, wegen $1 < \lambda \leqq 2$,

$$\left\{\begin{aligned} \left|\frac{1}{2\pi i}\int_{K_{[\lambda h]}} \frac{e^{\pi x}}{x^{h-m+1}F_{[\lambda h]}(x)}\,dx\right| &\leqq \frac{1}{2\pi}\cdot 2\pi[\lambda h]\,\frac{e^{[\lambda h]\pi}\,e^{2h}}{[\lambda h]^{h-m+1}\,h^{\lambda h}} \\ &\leqq \frac{e^{2(\pi+1)h}}{h^{(\lambda+1)h-m}}. \end{aligned}\right. \tag{44}$$

Aus (40), (42) und (44) folgt für $h > 4$

$$\begin{aligned} \left|\pi^h - \sum_{n=h}^{[\lambda h]} A_n F^{(h)}_{n-1}(0)\right| &\leqq \sum_{m=0}^{h}\frac{h!}{m!}\cdot\frac{([\lambda h]+1)!}{([\lambda h]-m+1)!}\, e^{c_{12}h}\, h^{\frac{1}{2}\lambda h-\frac{1}{2}m}\cdot\frac{e^{2(\pi+1)h}}{h^{(\lambda+1)h-m}} \\ &< h^{h+\frac{1}{2}\lambda h-(\lambda+1)h}\, e^{c_{12}h+2(\pi+1)h}\sum_{m=0}^{h}\frac{([\lambda h]+1)!}{m!([\lambda h]-m+1)!}\, h^{\frac{1}{2}m} \\ &\leqq h^{h+\frac{1}{2}\lambda h-(\lambda+1)h+\frac{1}{2}h}\, e^{c_{13}h}\,(1+1)^{[\lambda h]+1}, \end{aligned}$$

wegen $m \leqq h$ und mit $c_{13} = c_{12} + 2(\pi+1)$, also

$$< \left(\frac{e^{c_{14}}}{h^{\frac{\lambda-1}{2}}}\right)^h,$$

wegen $\lambda \leqq 2$.

Da $\left(\frac{e^{c_{14}}}{h^{\frac{\lambda-1}{2}}}\right)^h$ bei festem $\lambda (1 < \lambda \leqq 2)$ für $h \to \infty$ nach Null strebt, gibt es eine nur von λ abhängige positive Zahl $c_1' > 4$, derart daß für jede natürliche Zahl $h \geqq c_1'$

$$\left|\pi^h - \sum_{n=h}^{[\lambda h]} A_n F^{(h)}_{n-1}(0)\right| < \frac{\pi^h}{2}$$

ist, also

$$\left|\sum_{n=h}^{[\lambda h]} A_n F^{(h)}_{n-1}(0)\right| > \frac{\pi^h}{2}.$$

Im Intervall

$$h \leqq n \leqq \lambda h \qquad (h > c_2')$$

gibt es folglich wenigstens einen Wert n mit

$$|A_n F^{(h)}_{n-1}(0)| \geqq \frac{\pi^h}{2([\lambda h]-h+1)} \geqq \frac{\pi^h}{2(h+1)} \geqq \frac{\pi^4}{4h} > \frac{1}{h} \geqq \frac{1}{n},$$

wegen $1 < \lambda \leqq 2$, $\pi^4 > 4$ und $h \leqq n$.

Formel (41) mit h statt m und $n-1$ statt n ergibt deshalb

$$|A_n|\,\frac{n!\,(n-1)^{\frac{n-h}{2}}}{(n-h)!} > \frac{1}{n},$$

also wegen $h \leqq n \leqq \lambda h$ und $nn! \leqq n^n$

$$|A_n| > \frac{1}{n^n\, n^{\frac{n-\frac{n}{\lambda}}{2}}} = e^{-\frac{3\lambda-1}{2\lambda} n \log n},$$

womit (34) und also Hilfssatz 8 bewiesen ist.

Hilfssatz 9. *Jeder natürlichen Zahl n kann man ein Polynom mit ganzen Koeffizienten in* $\mathsf{K}(i)$

$$\mathrm{A}_n(x) = a_0 + a_1 x + \cdots + a_{m_1} x^{m_1} \tag{45}$$

von einem Grade m_1 mit

$$m_1 \leqq 2[\sqrt{n}] = m \tag{46}$$

zuordnen mit folgenden Eigenschaften:

Es ist

$$|a_\mu| < e^{c_{15} n} \qquad (\mu = 0, 1, 2, \ldots, m_1). \tag{47}$$

Ist λ irgendeine Zahl im Intervall $1 < \lambda \leqq 2$, so gibt es eine nur von λ abhängige positive Zahl $c_1' > 4$, derart daß für jede natürliche Zahl $h \geqq c_1'$ im Intervall

$$h \leqq n \leqq \lambda h$$

wenigstens ein n liegt mit

$$e^{-\frac{2\lambda-1}{2\lambda} n \log n - c_3 n} < |\mathrm{A}_n(e^{\pi})| < e^{-\frac{1}{2} n \log n + c_{14} n}, \tag{48}$$

wo c_3 die Konstante aus Hilfssatz 3 *ist.*

Beweis. Wir setzen

$$\mathrm{A}_n(x) = \sum_{\nu=0}^{n} (-1)^{J(\zeta_\nu)} \chi(n, \nu)\, x^{[\sqrt{n}] + R(\zeta_\nu)}, \tag{49}$$

wo $\chi(n, \nu)$ durch (19) definiert ist. Die Zahlen $J(\zeta_\nu)$ und $R(\zeta_\nu)$ sind ganz rational, während nach (10) $|\zeta_\nu| \leqq \sqrt{\nu} \leqq \sqrt{n}$, also $|(R(\zeta_\nu)| \leqq [\sqrt{n}]$ ist. $\mathrm{A}_n(x)$ ist folglich ein Polynom von einem Grade $\leqq 2[\sqrt{n}]$.

Nach Hilfssatz 6 ist $\chi(n, \nu)$ ganz im Körper $\mathsf{K}(i)$; nach den Formeln (21) und (22) desselben Hilfssatzes gilt außerdem

$$|\chi(n, \nu)| \leqq |\omega^2(n)| < e^{2c_9 n};$$

aus (45) und (49) folgt deshalb

$$|a_\mu| \leqq \sum_{\nu=0}^{n} |\chi(n, \nu)| < (n+1) e^{2c_9 n}, \qquad (\mu = 0, 1, \ldots, m_1),$$

so daß (47) mit $c_{15} = 2c_9 + 1$ bewiesen ist.

Nach (49) ist

$$\mathrm{A}_n(e^{\pi}) = \sum_{\nu=0}^{n} e^{\pi i J(\zeta_\nu)} \chi(n, \nu)\, e^{\pi[\sqrt{n}] + \pi R(\zeta_\nu)} = e^{\pi[\sqrt{n}]} \sum_{\nu=0}^{n} e^{\pi \zeta_\nu} \chi(n, \nu),$$

so daß aus (19) von Hilfssatz 6 und (31) von Hilfssatz 8 folgt:

$$\mathrm{A}_n(e^{\pi}) = e^{\pi[\sqrt{n}]} \omega(n)\, \varphi(n, 0) \sum_{\nu=0}^{n} \frac{e^{\pi \zeta_\nu}}{\varphi(n, \nu)} = e^{\pi[\sqrt{n}]} \omega(n)\, \varphi(n, 0) A_n. \tag{50}$$

Aus dem vorigen Hilfssatz folgt, daß für jede natürliche Zahl $h \geqq c_1' > 4$ (wo c_1' nur von λ abhängig ist) im Intervall $h \leqq n \leqq \lambda h$ mindestens ein n liegt mit

$$e^{-\frac{3\lambda-1}{2\lambda} n \log n} < A_n < e^{-n \log n + c_{11} n}. \tag{51}$$

Nach Hilfssatz 3 und Hilfssatz 6 folgt, da $\omega(n)$ eine ganze Zahl $\neq 0$ in $\mathsf{K}(i)$, also absolut $\geqq 1$ ist,

$$1 \cdot 1 \cdot e^{\frac{1}{2} n \log n - c_3 n} < |e^{\pi\sqrt{n}} \omega(n)\, \varphi(n, 0)| < e^{\pi n} \cdot e^{c_9 n} \cdot e^{\frac{1}{2} n \log n} = e^{\frac{1}{2} n \log n + c_{11} n}.$$

Wegen (50) und (51) folgt hieraus

$$e^{-\frac{3\lambda-1}{2\lambda}n\log n+\frac{1}{2}n\log n-c_{15}n} < |\mathrm{A}_n(e^{\pi})| < e^{-n\log n+c_{17}n+\frac{1}{2}n\log n+c_{18}n},$$

so daß (48) mit $c_{16} = c_{17} + c_{18}$ bewiesen ist. Hilfssatz 9 ist also bewiesen.

Hilfssatz 10. *Sind*

$$\mathrm{A}(x) = a_0 + a_1 x + \cdots + a_m x^m \qquad (m \geqq 1)$$

und

$$\mathrm{B}(x) = b_0 + b_1 x + \cdots + b_g x^g \qquad (g \geqq 1)$$

zwei Polynome mit ganzen Koeffizienten in $\mathsf{K}(i)$, *dann gibt es bekanntlich zwei Polynome* $\mathrm{P}(x)$ *und* $\mathrm{Q}(x)$ *mit ganzen Koeffizienten in* $\mathsf{K}(i)$ *von den Graden* $g-1$ *und* $m-1$, *derart daß*

$$\mathrm{A}(x)\,\mathrm{P}(x) + \mathrm{B}(x)\,\mathrm{Q}(x) = S \tag{52}$$

ist, wo S *die Resultante von* $\mathrm{A}(x)$ *und* $\mathrm{B}(x)$ *bezeichnet, also ganz in* $\mathsf{K}(i)$ *ist.*

Setzt man

$$\mathbf{Max}\,|a_\mu| = A \quad (\mu = 0, 1, \ldots, m) \quad \textit{und} \quad \mathbf{Max}\,|b_\gamma| = B \quad (\gamma = 0, 1, \ldots, g), \tag{53}$$

so gilt für diese Polynome $\mathrm{P}(x)$ *und* $\mathrm{Q}(x)$

$$|\mathrm{P}(x)| < \bar{c}_2(1 + |x|)^{g-1} A^{g-1} B^m e^{\bar{c}_1 m\log m} \tag{54}$$

und

$$|\mathrm{Q}(x)| < \bar{c}_2(1 + |x|)^{m-1} A^g B^{m-1} e^{\bar{c}_1 m\log m}, \tag{55}$$

wo $\bar{c}_1$ *und* $\bar{c}_2$ *nur von* g *abhängen* [11]).

Beweis. Es ist bekanntlich

$$S = \begin{vmatrix} a_0 & a_1 & a_2 & \cdots & a_m & & \\ & a_0 & a_1 & \cdots & a_{m-1} & a_m & \\ & & a_0 & \cdots & a_{m-2} & a_{m-1} & a_m \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & a_m \\ b_0 & b_1 & b_2 & \cdots & b_g & & \\ & b_0 & b_1 & \cdots & b_{g-1} & b_g & \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & b_g \end{vmatrix}, \tag{56}$$

$$\mathrm{P}(x) = \begin{vmatrix} 1 & a_1 & a_2 & \cdots & a_m & & \\ x & a_0 & a_1 & \cdots & a_{m-1} & a_m & \\ x^2 & 0 & a_0 & \cdots & a_{m-2} & a_{m-1} & a_m \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ x^{g-1} & \cdots & \cdots & \cdots & \cdots & \cdots & a_m \\ 0 & b_1 & b_2 & \cdots & b_g & & \\ 0 & 0 & b_1 & \cdots & b_{g-1} & b_g & \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & b_g \end{vmatrix},$$

und

$$\mathrm{Q}(x) = \begin{vmatrix} 0 & a_1 & a_2 & \cdots & a_m & & \\ 0 & a_0 & a_1 & \cdots & a_{m-1} & a_m & \\ 0 & 0 & a_0 & \cdots & a_{m-2} & a_{m-1} & a_m \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & a_m \\ 1 & b_1 & b_2 & \cdots & b_g & & \\ x & b_0 & b_1 & \cdots & b_{g-1} & b_g & \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ x^{m-1} & \cdots & \cdots & \cdots & \cdots & \cdots & b_g \end{vmatrix},$$

[11]) Die Zahlen $\bar{c}_1$, $\bar{c}_2$, $\bar{c}_3$, $\bar{c}_4$ und $\bar{c}_5$ bezeichnen in der Folge nur von g abhängige positive Zahlen.

wo die Determinanten die Ordnung $g + m$ haben. Setzt man

$$\mathrm{P}(x) = p_0 + p_1 x + \cdots + p_{g-1} x^{g-1} \tag{57}$$

und

$$\mathrm{Q}(x) = q_0 + q_1 x + \cdots + q_{m-1} x^{m-1}, \tag{58}$$

so folgt aus den Darstellungen von $\mathrm{P}(x)$ und $\mathrm{Q}(x)$ wegen (53)

$$|p_\gamma| \leqq (m + g - 1)!\, A^{g-1} B^m \qquad (\gamma = 0, 1, \ldots, g-1) \tag{59}$$

und

$$|q_\mu| \leqq (m + g - 1)!\, A^g B^{m-1} \qquad (\mu = 0, 1, \ldots, m-1). \tag{60}$$

Mit Rücksicht auf

$$(m + g - 1)! < (m + g)^{m+g} < \bar{c}_2 e^{\bar{c}_1 m \log m},$$

wo $\bar{c}_1$ und $\bar{c}_2$ geeignet gewählte nur von g abhängige positive Zahlen sind, folgt (54) aus (57) und (59), und (55) aus (58) und (60).

Hiermit ist Hilfssatz 10 bewiesen.

Hilfssatz 11. *Bezeichnen*

$$\mathrm{P}(x) = p_0 + p_1 x + \cdots + p_r x^r$$

und

$$\mathrm{Q}(x) = q_0 + q_1 x + \cdots + q_s x^s$$

irgend zwei Polynome; wird

$$\mathrm{T}(x) = t_0 + t_1 x + \cdots + t_{r+s} x^{r+s} = \mathrm{P}(x)\,\mathrm{Q}(x) \tag{61}$$

und weiter

$$P = \operatorname*{Max}_{\varrho=0,1,\ldots,r} |p_\varrho|, \qquad Q = \operatorname*{Max}_{\sigma=0,1,\ldots,s} |q_\sigma|, \qquad T = \operatorname*{Max}_{\tau=0,1,\ldots,r+s} |t_\tau| \tag{62}$$

gesetzt, dann gilt für $r + s \neq 0$

$$T \geqq \frac{1}{\{4(r+s)\}^r} PQ. \tag{63}$$

Beweis. Der Beweis wird bei beliebigem $s \geqq 1$ durch Schluß von r auf $r + 1$ geführt.

1. $r = 0$. Dann ist $T = PQ$, so daß (63) gültig ist.

2. $r = 1$. Wir setzen

$$\theta = \frac{1}{2s+2}. \tag{64}$$

Es gibt eine Zahl s_1 $(s_1 = 0, 1, \ldots, s)$, so daß

$$|q_{s_1}| = \operatorname*{Max}_{\sigma=0,1,\ldots,s} |q_\sigma| = Q \tag{65}$$

ist.

Wir unterscheiden jetzt zwei Fälle:

a) Es sei

$$|p_0| < (1 - \theta) P, \tag{66}$$

also $|p_1| = \mathrm{Max}\,(|p_0|, |p_1|) = P$. Setzt man noch $q_{s+1} = 0$, so ist

$$|t_{s_1+1}| = |p_0 q_{s_1+1} + p_1 q_{s_1}| \geqq |p_1 q_{s_1}| - |p_0 q_{s_1+1}|,$$

also wegen (65) und (66)

$$|T| \geqq |t_{s_1+1}| \geqq PQ - (1 - \theta)\, PQ = \theta PQ = \frac{1}{2s+2} PQ. \tag{67}$$

b) Es sei

(68) $$|p_0| \geqq (1-\theta)P.$$

Wir nehmen an, daß die Ungleichung

(69) $$T < \theta PQ$$

gilt.

Hieraus folgt dann, daß

(70) $$|q_{s_1-\sigma_1}| \geqq (1-2\sigma_1\theta)Q \qquad (\sigma_1 = 0, 1, \ldots, s_1)$$

ist. Denn für $\sigma_1 = 0$ ist dieses wegen (65) klar. Im Fall mit $\sigma_1 > 0$ sei die Ungleichung (70) mit $\sigma_1 - 1$ statt σ_1 schon bewiesen. Aus (69) folgt

$$|p_0 q_{s_1-\sigma_1+1} + p_1 q_{s_1-\sigma_1}| = |t_{s_1-\sigma_1+1}| \leqq T < \theta PQ,$$

also wegen (68) und wegen (70) mit $\sigma_1 - 1$ statt σ

$$\begin{aligned} P|q_{s_1-\sigma_1}| &\geqq |p_1 q_{s_1-\sigma_1}| \geqq |p_0 q_{s_1-\sigma_1+1}| - |p_0 q_{s_1-\sigma_1+1} + p_1 q_{s_1-\sigma_1}| \\ &\geqq (1-\theta)P \cdot (1-2(\sigma_1-1)\theta)Q - \theta PQ \geqq (1-2\sigma_1\theta)PQ, \end{aligned}$$

so daß (70) bewiesen ist.

Wenden wir (70) mit $\sigma_1 = s_1$ an, so kommt

$$|q_0| \geqq (1-2s_1\theta)Q,$$

also wegen (68)

$$T \geqq |t_0| = |p_0 q_0| \geqq (1-\theta)P \cdot (1-2s_1\theta)Q \geqq \{1-(2s_1+1)\theta\}PQ,$$

folglich mit Rücksicht auf (64)

$$T \geqq \left(1 - \frac{2s_1+1}{2s+2}\right) PQ \geqq \frac{1}{2s+2} PQ = \theta PQ.$$

Die Ungleichung (69) führt also zu einem Widerspruch. Es ist somit im Fall b)

(71) $$T \geqq \theta PQ = \frac{1}{2s+2} PQ.$$

Wegen (67) gilt diese Ungleichung also allgemein im Fall mit $r = 1$. Hieraus folgt (63) mit $r = 1$

3) $r > 1$. Es sei Hilfssatz 11 mit $r-1$ statt r schon bewiesen. Wir setzen jetzt

(72) $$\begin{cases} \mathrm{P}(x) = p_0 + p_1 x + \cdots + p_r x^r = (p+x)\,(p_0^* + p_1^* x + \cdots + p_{r-1}^* x^{r-1}) \\ \qquad\quad = (p+x)\,\mathrm{P}^*(x), \end{cases}$$

so daß $-p$ irgendeine Nullstelle des Polynoms $\mathrm{P}(x)$ ist. Man setze

$$\mathrm{T}^*(x) = t_0^* + t_1^* x + \cdots + t_{r+s-1}^* x^{r+s-1} = \mathrm{P}^*(x)\,\mathrm{Q}(x),$$

$$P^* = \operatorname*{Max}_{\varrho=0,1,\ldots,r-1} |p_\varrho^*| \qquad \text{und} \qquad T^* = \operatorname*{Max}_{\tau=0,1,\ldots,r+s-1} |t_\tau^*|.$$

Aus (72) folgt dann unmittelbar

(73) $$P \leqq 2\,\mathrm{Max}\,(|p|, 1) \cdot P^*.$$

Wir wenden Hilfssatz 11 an mit $\mathrm{P}^*(x)$ statt $\mathrm{P}(x)$, also mit $r-1$ statt r und mit P^* statt P, T^* statt T, und finden dann

(74) $$T^* \geqq \frac{1}{\{4(r-1+s)\}^{r-1}} P^*Q > \frac{1}{\{4(r+s)\}^{r-1}} P^*Q.$$

Es ist $\mathrm{T}(x) = (p+x)\,\mathrm{T}^*(x)$; wir können deshalb Fall 2 anwenden mit $p+x$ statt $\mathrm{P}(x)$, $\mathrm{T}^*(x)$ statt $\mathrm{Q}(x)$ und mit $r+s-1$ statt s. Nach (71) ist somit

$$T \geqq \frac{1}{2(r+s-1)+2} \cdot \mathrm{Max}\,(|p|, 1) \cdot T^*,$$

also nach (74) und (73)

$$T \geqq \frac{1}{2(r+s)} \cdot \mathrm{Max}\,(|p|, 1) \cdot \frac{P^*Q}{\{4(r+s)\}^{r-1}} \geqq \frac{1}{\{4(r+s)\}^{r}} PQ,$$

womit (63) bewiesen ist.

Hilfssatz 12. *Bezeichnet ε eine positive Zahl,*

(75) $$\mathrm{B}(x) = b_0 + b_1 x + \cdots + b_g x^g$$

ein irreduzibles Polynom mit ganzen Koeffizienten in $\mathrm{K}(i)$, *das nicht identisch verschwindet, und wird*

(76) $$B = \mathop{\mathrm{Max}}_{\gamma=0,1,\ldots,g} (|b_\gamma|; 3)$$

gesetzt, so kann man eine nur von g und ε abhängige positive Zahl α_1 finden, so daß

(77) $$|\mathrm{B}(e^{\pi})| > \alpha_1 B^{-(4+\varepsilon)\frac{\log B}{\log\log B}}$$

ist [12]).

Beweis. Erster Schritt. Ohne Beschränkung der Allgemeinheit können wir annehmen, daß

$$\varepsilon < 1$$

und daß

$$g \geqq 1$$

ist.

Wir setzen

(78) $$\lambda = 1 + \delta, \quad \lambda_1 = 1 + 2\delta, \quad \text{wo} \quad \delta = \frac{\varepsilon}{52} \text{ ist;}$$

ferner

(79) $$t = (2 + 6\delta)^2 \frac{\log^2 B}{(\log\log B)^2},$$

und ziehen aus (78) und (79) einige Folgerungen.

I. Aus (79) folgt für $B > \alpha_2$

$$t > \log^2 B \cdot \frac{1}{(\log\log B)^2} > (\log B)^{2(1-\delta)},$$

d. h.

$$\log\log B < \frac{\log t}{2(1-\delta)},$$

so daß für $B > \alpha_3 \geqq \alpha_2$ aus (79) hervorgeht:

(80) $$\log B = \frac{\sqrt{t}}{2(1+3\delta)} \log\log B < \frac{\sqrt{t} \cdot \log t}{4(1+3\delta)(1-\delta)} = \frac{\sqrt{t} \cdot \log t}{4(1+2\delta-3\delta^2)} < \frac{\sqrt{t} \cdot \log t}{4(1+\delta)},$$

weil wegen (78) gilt $3\delta^2 < \frac{3}{52} \cdot \delta < \delta$.

Wir setzen jetzt

(81) $$\bar{c}_3 = 4\bar{c}_1 + c_{15} g + g \log(1 + e^{\pi}) + \log \bar{c}_2, \qquad \bar{c}_4 = c_{16} + \bar{c}_3,$$

wo c_{15} und c_{16} die Zahlen aus Hilfssatz 9 sind, $\bar{c}_1$ und $\bar{c}_2$ die Zahlen aus Hilfssatz 10, welche nur von g abhängen, und wo $\bar{c}_2 \geqq 1$ ist. Folglich hängen $\bar{c}_3$ und $\bar{c}_4$ nur von g ab, und es gilt $\bar{c}_4 > \bar{c}_3 > 0$. Für $B > \alpha_4 \geqq \alpha_3$ folgt nun aus (79) und (80) leicht

(82) $$2\log B - \frac{1}{2}\sqrt{t} \cdot \log t + 2\bar{c}_4\sqrt{t} < 2\log B - \frac{1}{2+2\delta}\sqrt{t}\log t - 1 < -1.$$

II. Wenn $\bar{c}_3$ durch (81) definiert ist, so ist klar, daß für $B > \alpha_5$ gilt:

(83) $$\frac{(2\bar{c}_3 + 2)(2 + 6\delta)}{\log\log B} < 2\delta.$$

---

[12]) Hier, wie in der Folge, bezeichnen $\alpha_1, \alpha_2, \ldots, \alpha_{19}$ geeignet gewählte positive Zahlen, die nur von ε und g abhängen.

Aus (78) und (79) folgt

$$2\sqrt{\lambda_1}\sqrt{t}\log B + (2\bar{c}_3 + 2)t$$
$$= 2\sqrt{1+2\delta}\cdot(2+6\delta)\frac{\log^2 B}{\log\log B} + (2\bar{c}_3+2)(2+6\delta)^2\frac{\log^2 B}{(\log\log B)^2},$$

also, wegen (83) und $\sqrt{1+2\delta} < 1+\delta$, für $B > \alpha_5$

$$< 4(1+2\delta)(1+3\delta)\frac{\log^2 B}{\log\log B} = 4(1+5\delta+6\delta^2)\frac{\log^2 B}{\log\log B}.$$

Aus (78) folgt $6\delta^2 < \frac{6}{5^2}\delta < \delta$, also $4(1+5\delta+6\delta^2) < 4+24\delta < 4+\varepsilon$, so daß wir für $B > \alpha_5$ haben:

$$2\sqrt{\lambda_1}\sqrt{t}\log B + (2\bar{c}_3+2)t < (4+\varepsilon)\frac{\log^2 B}{\log\log B}. \tag{84}$$

III. Für $B > \alpha_6$ geht aus (79) hervor: $t < \log^2 B$, d. h.

$$\log t < 2\log\log B,$$

so daß aus (78) und (79) folgt:

$$\begin{cases} \dfrac{2\lambda_1 - 1 + \delta}{2} t\log t < \dfrac{1+5\delta}{2}(2+6\delta)^2\dfrac{\log^2 B}{(\log\log B)^2}\cdot 2\log\log B \\ \qquad = 4(1+5\delta)(1+3\delta)^2\dfrac{\log^2 B}{\log\log B}. \end{cases} \tag{85}$$

Aus (78) folgt $\delta = \frac{1}{5^2}\varepsilon < \frac{1}{5^2}$, also

$$4(1+5\delta)(1+3\delta)^2 = 4(1+5\delta)(1+6\delta+9\delta^2) < 4(1+5\delta)(1+7\delta)$$
$$= 4(1+12\delta+35\delta^2) < 4+52\delta = 4+\varepsilon.$$

Aus (85) geht also für $B > \alpha_6$ hervor:

$$\frac{2\lambda_1 - 1 + \delta}{2} t\log t < (4+\varepsilon)\frac{\log^2 B}{\log\log B}. \tag{86}$$

IV. Für $B > \alpha_7$ ist wegen (78) und (79)

$$\log t > 2c_{16}, \quad \delta t > 2,$$

wo c_{16} die positive absolute Konstante von Hilfssatz 9 ist, und also

$$\lambda(t+1) < (1+\delta)t + 2 < (1+2\delta)t = \lambda_1 t.$$

Nach der letzten Ungleichung gibt es also wenigstens eine natürliche Zahl h mit

$$t \leqq h < \lambda h \leqq \lambda_1 t.$$

Wählen wir für die in Hilfssatz 9 genannte Zahl λ, die in (78) definierte Größe, so hängt, die in diesem letzten Hilfssatz genannte Zahl $c_1' > 4$ nur von ε und g ab. Es gibt also nach der Definition von t in (79) ein $\alpha_8 \geqq \alpha_7$, so daß für $B > \alpha_8$ gilt $h \geqq t > c_1' > 4$.

Hilfssatz 9 lehrt uns nun folgendes:
Für $B > \alpha_8$ liegt im Intervall

$$h \leqq n \leqq \lambda h,$$

also erst recht im Intervall

$$t \leqq n \leqq \lambda_1 t \tag{87}$$

wenigstens eine natürliche Zahl n, zu der ein durch (45) definiertes Polynom $A_n(x)$ vom Grade

$$m_1 \leqq 2[\sqrt{n}] = m \tag{88}$$

mit ganzen Koeffizienten in $\mathsf{K}(i)$ angebbar ist mit

$$\bar{A}_n = \operatorname*{Max}_{\mu=0,1,\ldots,m_1} |a_\mu| < e^{c_{18}n} \tag{89}$$

und wegen $\lambda_1 > \lambda$ mit

$$e^{-\frac{2\lambda_1-1}{2\lambda_1} n\log n - c_{15} n} < |A_n(e^\pi)| < e^{-\frac{1}{2} n\log n + c_{16} n}. \tag{90}$$

Aus $n \geqq t$ und $\log t > 2c_{16}$ folgt

$$-\tfrac{1}{2} n\log n + c_{16} n < 0,$$

also gilt

$$0 < |A_n(e^\pi)| < 1.$$

Im Fall mit $m_1 = 0$ ist $A_n(x)$ für jedes x, also auch für $x = e^\pi$, eine ganze Zahl in $K(i)$. Das widerspricht aber der letzten Ungleichung, so daß

$$m_1 \geqq 1$$

ist.

Zweiter Schritt. Es sei

$$B(x) \neq A_n(x).$$

Wir wenden Hilfssatz 10 an mit $A_n(x)$ statt $A(x)$, also mit m_1 statt m und $\bar{A}_n$ statt A; außerdem können wir den Ausdruck B in (53) ersetzen durch den Ausdruck B in (76), weil in (54) und (55) die rechten Glieder dadurch majorisiert werden.

Wegen $m_1 \geqq 1$ und $g \geqq 1$ sind die Bedingungen von Hilfssatz 10 erfüllt. Es gibt folglich zwei Polynome $P(x)$ und $Q(x)$ mit ganzen Koeffizienten in $K(i)$, so daß

$$A_n(x)P(x) + B(x)Q(x) = S \tag{91}$$

eine ganze Zahl $\neq 0$ in $K(i)$ ist; dabei gilt

$$|P(x)| < \bar{c}_2 (1 + |x|)^{g-1} \bar{A}_n^{g-1} B^{m_1} e^{\bar{c}_1 m_1 \log m_1}, \tag{92}$$

$$|Q(x)| < \bar{c}_2 (1 + |x|)^{m_1-1} \bar{A}_n^{g} B^{m_1-1} e^{\bar{c}_1 m_1 \log m_1}, \tag{93}$$

wo $\bar{c}_1$ und $\bar{c}_2$ nur von g abhängen.

Es ist wegen (87) $n \geqq t > c_1' > 4$, also folgt aus (88) und (89)

$$\begin{aligned}\bar{c}_2(1 + e^\pi)^{mg} \bar{A}_n^{g} B^{m} e^{\bar{c}_1 m\log m} &< B^{2\sqrt{n}} e^{2\sqrt{n}\cdot g\cdot\log(1+e^\pi) + \log\bar{c}_2 + c_{15} ng + 2\bar{c}_1\sqrt{n}\log n + 2\bar{c}_1\sqrt{n}\log 2} \\ &< B^{2\sqrt{n}} e^{n\{c_{15}g + 4\bar{c}_1 + g\log(1+e^\pi) + \log\bar{c}_2\}} = B^{2\sqrt{n}} e^{\bar{c}_3 n},\end{aligned}$$

wegen (81). Wegen $m_1 \geqq 1$, $g \geqq 1$, $m_1 \leqq m$ folgt deshalb aus (92) und (93)

$$|P(e^\pi)| < B^{2\sqrt{n}} e^{\bar{c}_3 n}, \tag{94}$$

$$|Q(e^\pi)| < B^{2\sqrt{n}} e^{\bar{c}_3 n}. \tag{95}$$

Aus (94) und (90) folgt nun für $B > \alpha_8$

$$|P(e^\pi)\, A_n(e^\pi)| < B^{2\sqrt{n}} e^{\bar{c}_3 n - \frac{1}{2} n\log n + c_{14} n} = e^{2\sqrt{n}\log B - \frac{1}{2} n\log n + \bar{c}_4 n},$$

wegen (81). Wir finden also wegen (87) und $\lambda_1 < 2$

$$|P(e^\pi)\, A_n(e^\pi)| < e^{\sqrt{n}\{2\log B - \frac{1}{2}\sqrt{t}\log t + 2\bar{c}_4\sqrt{t}\}},$$

also für $B > \alpha_9 = \mathrm{Max}\,(\alpha_4, \alpha_8)$ wegen (82) und $n \geqq 1$

$$< e^{-\sqrt{n}} < \tfrac{1}{2}.$$

Aus $|S| \geqq 1$ und (91) folgt also für $B > \alpha_9$

$$|B(e^\pi)\, Q(e^\pi)| \geqq 1 - |P(e^\pi)\, A_n(e^\pi)| > 1 - \tfrac{1}{2} = \tfrac{1}{2},$$

oder wegen (95) und $n \geqq 1$

$$|B(e^\pi)| > \tfrac{1}{2} B^{-2\sqrt{n}} e^{-\bar{c}_3 n} > e^{-2\sqrt{n}\log B - (\bar{c}_3+1)n}.$$

Aus (87) und (78) folgt $n \leqq \lambda_1 t$ und $n < 2t$, also für $B > \alpha_9$

$$|B(e^\pi)| < e^{-2\sqrt{\lambda_1}\sqrt{t}\log B - (2\bar{c}_3+2)t},$$

d. h. für $B > \alpha_{10} = \mathrm{Max}\,(\alpha_9, \alpha_5)$ wegen (84)

$$|B(e^\pi)| > e^{-(4+\varepsilon)\frac{\log^2 B}{\log\log B}}. \tag{96}$$

Dritter Schritt. *Es sei*

$$B(x) \mid A_n(x),$$

dann gibt es ein Polynom

$$D(x) = d_0 + d_1 x + \cdots + d_{m_1-g} x^{m_1-g}$$

mit

$$D = \operatorname*{Max}_{\tau=0,1,\ldots,m_1-g} |d_\tau|,$$

so daß

$$A_n(x) = B(x)\, D(x) \tag{97}$$

ist. Nach Hilfssatz 11 mit $B(x)$ statt $P(x)$, $D(x)$ statt $Q(x)$ und $A_n(x)$ statt $T(x)$ gilt somit, da $m_1 \neq 0$ ist,

$$\bar{A}_n \geqq \frac{1}{(4m_1)^g} BD.$$

Weil die Koeffizienten von $B(x)$ ganz in $K(i)$ sind und $B(x)$ nicht identisch verschwindet, gilt $|B| \geqq 1$, also

$$D \leqq (4m_1)^g \bar{A}_n < e^{8gn + c_{15}n}, \tag{98}$$

wegen (88), $2\sqrt{n} \leqq 2n$ für $n \geqq 1$ und (89).

Wir haben also wegen $g \geqq 1$ und (88)

$$|D(e^{\pi})| < (m_1 - g + 1)\, D e^{\pi(m_1-g)} < 2\sqrt{n}\, e^{(8g + c_{15})n + \pi \cdot 2\sqrt{n}} < e^{(2 + 8g + c_{15} + 2\pi)n}.$$

Aus (97) geht also hervor

$$|B(e^{\pi})| = \frac{|A_n(e^{\pi})|}{|D(e^{\pi})|} > |A_n(e^{\pi})|\, e^{-(2 + 8g + c_{15} + 2\pi)n},$$

also wegen (90) für $B > \alpha_8$

$$|B(e^{\pi})| > e^{-\frac{2\lambda_1 - 1}{2\lambda_1} n \log n - (c_3 + 2 + 8g + c_{15} + 2\pi)n} > e^{-\frac{2\lambda_1 - 1}{2} t \log t - \left(\frac{2\lambda_1 - 1}{2} \log 2 + 2c_3 + 4 + 16g + 2c_{15} + 4\pi\right) t},$$

weil (87) gilt und weil $\lambda_1 < 2$ ist. Wegen (79) für $B > \alpha_{11} \geqq \alpha_8$ kann man also schließen:

$$|B(e^{\pi})| < e^{-\frac{2\lambda_1 - 1 + \delta}{2} t \log t},$$

also für $B > \operatorname{Max}(\alpha_6, \alpha_{11}) = \alpha_{12}$ wegen (86)

$$|B(e^{\pi})| > e^{-(4+\varepsilon)\frac{\log^2 B}{\log\log B}}. \tag{99}$$

Vierter Schritt. Setzt man

$$\alpha_{13} = \operatorname{Max}(3, \alpha_{10}, \alpha_{12}), \quad \alpha_{14} = [\alpha_{13} + 1] \tag{100}$$

und

$$\alpha_1 = \frac{1}{\alpha_{14}}\, e^{-(4+\varepsilon)\frac{\log^2 \alpha_{14}}{\log\log 3}}, \tag{101}$$

so hängt die positive Zahl α_1 nur von ε und g ab, und es gilt $\alpha_1 < 1$.

Zum Beweise von (77) unterscheiden wir jetzt zwei verschiedene Fälle.

1. Es sei im Polynom

$$B(x) = b_0 + b_1 x + \cdots + b_g x^g$$

die Zahl

$$B = \operatorname*{Max}_{\gamma=0,1,\ldots,g} (|b_\gamma|, 3) \geqq \alpha_{13}.$$

Der zweite und dritte Schritt lehren uns wegen (96) oder (99), (100) und $\alpha_1 < 1$ unmittelbar, daß (77) gilt.

2. Es sei

$$B < \alpha_{13}. \tag{102}$$

Dann hat das Polynom mit ganzen Koeffizienten in $\mathsf{K}(i)$

$$\alpha_{14}\mathrm{B}(x) = \alpha_{14}b_0 + \alpha_{14}b_1 x + \cdots + \alpha_{14}b_g x^g$$

wegen (100) die Eigenschaft, daß

$$B' = \mathrm{Max}\,(\alpha_{14}\,|b_\gamma|, 3) \geqq \alpha_{14} > \alpha_{13} \tag{103}$$

ist; außerdem gilt wegen (102) und $\alpha_{13} \geqq 3$

$$3 \leqq B' < \alpha_{13}\,\alpha_{14} < \alpha_{14}^2\,, \tag{104}$$

wegen (100). Je nachdem $\alpha_{14}\mathrm{B}(x) \neq \mathrm{A}_n(x)$ oder $\alpha_{14}\mathrm{B}(x) \equiv \mathrm{A}_n(x)$ wenden wir die Resultate von Schritt 2 oder von Schritt 3 an mit $\alpha_{14}\mathrm{B}(x)$ statt $\mathrm{B}(x)$ und B' statt B. Es lehren uns (96) und (99) wegen (103) und (100)

$$|\alpha_{14}\mathrm{B}(e^{\pi})| > e^{-(4+\varepsilon)\frac{\log^2 B'}{\log\log B'}} > e^{-(4+\varepsilon)\frac{\log^2 \alpha_{14}^2}{\log\log 3}}$$

wegen (104), also wegen (101) und $B \geqq 3$

$$|\mathrm{B}(e^{\pi})| > \alpha_1, \quad \text{d. h.} \quad > \alpha_1 e^{-(4+\varepsilon)\frac{\log^2 B}{\log\log B}}.$$

Auch im letzten Fall ist (77) also bewiesen.

Hilfssatz 13. *Es seien* $\mathrm{B}(x)$ *und* $\mathrm{B}_\varrho(x)$ $(\varrho = 1, 2, \ldots, r)$ *Polynome*:

$$\mathrm{B}(x) = b_0 + b_1 x + \cdots + b_g x^g,$$
$$\mathrm{B}_\varrho(x) = b_{\varrho,0} + b_{\varrho,1} x + \cdots + b_{\varrho,g_\varrho} x^{g_\varrho} \qquad (\varrho = 1, 2, \ldots, r),$$

mit

$$\mathrm{B}(x) = \mathrm{B}_1(x)\,\mathrm{B}_2(x) \cdots \mathrm{B}_r(x)$$

und

$$B = \max_{\gamma=0,1,\ldots,g} |b_\gamma|, \qquad B_\varrho = \max_{\gamma=0,1,\ldots,g_\varrho} |b_{\varrho,\gamma}| \qquad (\varrho = 1, 2, \ldots, r)\,,$$

dann besteht die Ungleichung

$$B \geqq \frac{1}{(4g)^g} B_1 B_2 \cdots B_r \text{ [13]}. \tag{105}$$

Beweis. Für $r = 1$ ist dieser Satz evident. Es sei also $r > 1$, und der Satz mit $r - 1$ statt r schon bewiesen. Setzen wir also

$$\overline{\mathrm{B}}(x) = \overline{b_0} + \overline{b_1} x + \cdots + \overline{b_{\bar g}}\, x^{\bar g} = \mathrm{B}_2(x)\,\mathrm{B}_3(x) \cdots \mathrm{B}_r(x)$$

und

$$\overline{B} = \max_{\gamma=0,1,\ldots,\bar g} |\overline{b_\gamma}|\,,$$

so gilt folglich

$$\overline{B} \geqq \frac{1}{(4\bar g)^{\bar g}} B_2 B_3 \cdots B_r\,. \tag{106}$$

Es ist aber

$$\mathrm{B}(x) = \mathrm{B}_1(x)\overline{\mathrm{B}}(x),$$

so daß nach Hilfssatz 11 mit $\mathrm{B}_1(x)$ statt $\mathrm{P}(x)$ und $\overline{\mathrm{B}}(x)$ statt $\mathrm{Q}(x)$, also mit $\mathrm{B}(x)$ statt $\mathrm{T}(x)$, g_1 statt r und $\bar g$ statt s

$$B \geqq \frac{1}{(4g)^{g_1}} B_1 \overline{B} \text{ [13]}$$

ist.

Nach (106) gilt deshalb wegen $g = g_1 + \bar g \geqq \bar g$

---

[13]) Ist a irgendeine Zahl, so setze man $a^0 = 1$.

$$B \geqq \frac{1}{(4g)^{g_1}} \cdot \frac{1}{(4\bar{g})^{\bar{g}}} B_1 B_2 \cdots B_r \geqq \frac{1}{(4g)^{g_1+\bar{g}}} B_1 B_2 \cdots B_r = \frac{1}{(4g)^{g}} B_1 B_2 \cdots B_r ,$$

womit Hilfssatz 13 bewiesen ist.

Beweis des Satzes [14]). Wir zerlegen $\mathrm{B}(x)$ in seine in $\mathsf{K}(i)$ irreduziblen Faktoren:

$$\mathrm{B}_\varrho(x) = b_{\varrho,0} + b_{\varrho,1}\, x + \cdots + b_{\varrho,g_\varrho}\, x^{g_\varrho} \qquad (\varrho = 1, 2, \ldots, r) ,$$

wobei die Koeffizienten $b_{\varrho,\gamma}$ $(\gamma = 1, 2, \ldots, g_\varrho)$ ganz in $\mathsf{K}(i)$ sind, so daß

$$\mathrm{B}(x) = \mathrm{B}_1(x)\, \mathrm{B}_2(x) \cdots \mathrm{B}_r(x)$$

ist. Es sei

$$B'_\varrho = \operatorname*{Max}_{\gamma=0,1,\ldots,g_\varrho} (27\,|\,b_{\varrho,\gamma}\,|) \qquad (\varrho = 1, 2, \ldots, r);$$

also erst recht

$$B'_\varrho > 3 .$$

Nach Hilfssatz 12 gilt deshalb

$$|\,27\,\mathrm{B}_\varrho(e^{\pi})| > C^{(\varrho)}\, e^{-\left(4+\frac{\varepsilon}{2}\right)\frac{\log^2 B'_\varrho}{\log\log B'_\varrho}} \qquad (\varrho = 1, 2, \ldots, r),$$

wo $C^{(\varrho)} > 0$ nur von g_ϱ und ε abhängt. Wegen $g = g_1 + g_2 + \cdots + g_r$ gibt es folglich eine allein von g und ε abhängige positive Zahl $\alpha_{15} < 1$ mit

$$|\,\mathrm{B}_\varrho(e^{\pi})| > \alpha_{15}\, e^{-\left(4+\frac{\varepsilon}{2}\right)\frac{\log^2 B'_\varrho}{\log\log B'_\varrho}} \qquad (\varrho = 1, 2, \ldots, r). \tag{107}$$

Die Funktion $\dfrac{x}{\log x}$ ist für $x > e$ monoton wachsend, deshalb gilt für r beliebige Zahlen $x_\varrho > e$ $(\varrho = 1, 2, \ldots, r)$

$$\begin{aligned}\frac{x_1^2}{\log x_1} + \frac{x_2^2}{\log x_2} + \cdots + \frac{x_r^2}{\log x_r} &< x_1 \frac{x_1 + x_2 + \cdots + x_r}{\log (x_1 + x_2 + \cdots + x_r)} \\ &+ x_2 \frac{x_1 + x_2 + \cdots + x_r}{\log (x_1 + x_2 + \cdots + x_r)} + \cdots + x_r \frac{x_1 + x_2 + \cdots + x_r}{\log (x_1 + x_2 + \cdots + x_r)} \\ &= \frac{(x_1 + x_2 + \cdots + x_r)^2}{\log (x_1 + x_2 + \cdots + x_r)} .\end{aligned}$$

Wegen $B'_\varrho \geqq 27 = 3^3 > e^e$ dürfen wir hierin für x_ϱ die Zahl $\log B'_\varrho$ einsetzen $(\varrho = 1, 2, \ldots, r)$, so daß

$$\frac{\log^2 B'_1}{\log\log B'_1} + \frac{\log^2 B'_2}{\log\log B'_2} + \cdots + \frac{\log^2 B'_r}{\log\log B'_r} < \frac{\log^2 (B'_1 B'_2 \cdots B'_r)}{\log\log (B'_1 B'_2 \cdots B'_r)} \tag{108}$$

ist.

Es ist nun $27^r\,\mathrm{B}(x) = 27\,\mathrm{B}_1(x) \cdot 27\,\mathrm{B}_1(x) \cdots 27\,\mathrm{B}_r(x)$. Wir wenden jetzt deshalb Hilfssatz 13 an mit $27\,\mathrm{B}_\varrho(x)$ statt $\mathrm{B}_\varrho(x)$ $(\varrho = 1, 2, \ldots, r)$, $27^r\,\mathrm{B}(x)$ statt $\mathrm{B}(x)$, und also mit B'_ϱ statt B_ϱ $(\varrho = 1, 2, \ldots, r)$, und mit

$$B' = \operatorname*{Max}_{\gamma=0,1,\ldots,g} (27^r\,|\,b_\gamma|)$$

statt B. Ungleichung (105) ergibt dann wegen $B' \leqq 27^r B \leqq 27^g B$

$$B'_1 B'_2 \cdots B'_r < (4g)^g B' \leqq (4 \cdot 27\, g)^g B = \bar{c}_5 B,$$

wo $\bar{c}_5$ eine nur von g abhängige Zahl $\geqq 1$ ist. Da die Funktion $\dfrac{x^2}{\log x} = x \cdot \dfrac{x}{\log x}$ für $x > e$ monoton wächst, folgt also aus (108)

$$\frac{\log^2 B'_1}{\log\log B'_1} + \frac{\log^2 B'_2}{\log\log B'_2} + \cdots + \frac{\log^2 B'_r}{\log\log B'_r} < \frac{\log^2 (\bar{c}_5 B)}{\log\log B} .$$

Aus (107) geht folglich hervor:

---

[14]) Man beachte Bemerkung 1.

$$|\mathrm{B}(e^\pi)| = |\mathrm{B}_1(e^\pi)\,\mathrm{B}_2(e^\pi)\cdots\mathrm{B}_r(e^\pi)| > \alpha_{15}^r\, e^{-\left(4+\frac{\varepsilon}{2}\right)\sum_{\varrho=1}^{r}\frac{\log^2 B_\varrho'}{\log\log B_\varrho'}}$$
$$> \alpha_{15}^g\, e^{-\left(4+\frac{\varepsilon}{2}\right)\frac{\log^2(\bar{c}_5 B)}{\log\log B}}.$$

Es gibt eine nur von ε und g abhängige positive Zahl α_{16}, so daß für $B > \alpha_{16}$

$$\left\{1+\frac{\log \bar{c}_5}{\log B}\right\}^2 < \frac{4+\varepsilon}{4+\frac{\varepsilon}{2}}$$

ist, also

$$\left(4+\frac{\varepsilon}{2}\right)\log^2(\bar{c}_5 B) < (4+\varepsilon)\log^2 B,$$

so daß dann

$$|\mathrm{B}(e^\pi)| > \alpha_{15}^g\, e^{-(4+\varepsilon)\frac{\log^2 B}{\log\log B}} \tag{109}$$

ist.

Im Fall $B \leqq \alpha_{16}$ gibt es zu jedem g wegen

$$\mathrm{B}(e^\pi) \neq 0$$

eine nur von ε und g abhängige positive Zahl α_{17} mit

$$|\mathrm{B}(e^\pi)| > \alpha_{17} > \alpha_{17}\, e^{-(4+\varepsilon)\frac{\log^2 B}{\log\log B}}, \tag{110}$$

wegen $B \geqq 3$.

Wegen (109) und (110) ist somit der Satz bewiesen, wobei

$$C = \mathrm{Min}\,(\alpha_{15}^g, \alpha_{17})$$

gesetzt wurde.

Beweis der Richtigkeit von Bemerkung 2 bei dem Satz. Diese Bemerkung ist trivial, wenn

$$|e^\pi - \theta| > 1$$

ist, weil man dann in (4) nur $\bar{C} < 1$ zu wählen braucht. Es sei also angenommen

$$|e^\pi - \theta| \leqq 1.$$

Dann ist

$$|\mathrm{B}(e^\pi)| = |\mathrm{B}(e^\pi) - \mathrm{B}(\theta)| = |\sum_{\gamma=0}^{g} b_\gamma (e^{\pi\gamma} - \theta^\gamma)|$$
$$\leqq |e^\pi - \theta|\,(g+1)\,(e^\pi+1)^{g-1} B,$$

d. h. wegen (3) mit $\frac{\varepsilon}{2}$ statt ε

$$|e^\pi - \theta| > \frac{C}{(g+1)\,(e^\pi+1)^{g-1}}\, B^{-\left(4+\frac{\varepsilon}{2}\right)\frac{\log B}{\log\log B}-1}. \tag{111}$$

Es gibt eine nur von g und ε abhängige Zahl α_{18}, so daß für $B > \alpha_{18}$ aus (111) folgt:

$$|e^\pi - \theta| > B^{-(4+\varepsilon)\frac{\log B}{\log\log B}}. \tag{112}$$

Andernfalls ist $B \leqq \alpha_{18}$. Da θ algebraisch und nach dem Satze e^π transzendent ist, hat man zu jedem $g \geqq 0$ eine nur von g und α_{18} abhängige Zahl α_{19} mit

$$|e^\pi - \theta| > \alpha_{19}, \text{ also } > \alpha_{19} B^{-(4+\varepsilon)\frac{\log B}{\log\log B}}, \tag{113}$$

wegen $B \geqq 3$. Aus (112) und (113) folgt (4) mit etwa

$$\bar{C} = \mathrm{Min}\,(1, \alpha_{19}).$$

Eingegangen 21. Dezember 1931.

Ein Satz über die Zerlegung von Primzahlen bestimmter arithmetischer Progressionen in algebraischen Zahlkörpern.

Von *U. Wegner* in Darmstadt.

Satz: *In jedem algebraischen Zahlkörper* $\mathsf{P}(\vartheta)$ *über* P, *dem Körper der rationalen Zahlen, vom Primzahlgrad* p *gibt es unendlich viele Primzahlen der Form* $px+1$, *die in* $\mathsf{P}(\vartheta)$ *selbst Primideale sind.*

Beweis: Man kann offenbar $p \neq 2$ annehmen. $f(x)=0$ sei die algebraische Gleichung p-ten Grades über P und daselbst irreduzibel, die $\mathsf{P}(\vartheta)$ erzeugt. Es sei $g(x)=x^{p-1}+\cdots+x+1=0$. $h(x)=f(x)\cdot g(x)=0$ besitzt dann eine Galoissche Permutationsgruppe $\mathfrak{G}_h$, die sich aus

$$\mathfrak{G}_f=\{E=S_1, S_2, \ldots, S_{p\cdot m}\} \quad \text{und} \quad \mathfrak{G}_g=\{E=T_1, T_2, \ldots, T_{p-1}\}$$

zu

$$\mathfrak{G}_k=\{S_{\nu_1}\cdot T_{\nu_1}, S_{\nu_2}\cdot T_{\nu_2}, \ldots, S_{\nu_n}\cdot T_{\nu_n}\}$$

zusammensetzt, wobei die S_{ν_ϱ} alle Permutationen von $\mathfrak{G}_f$ durchlaufen, aber vielleicht mehrfach; analog die T_{ν_ϱ}. Die verschiedenen Permutationen $S_{\nu_\varkappa}$, die in $\mathfrak{G}_h$ an die Permutation E von $\mathfrak{G}_g$ gekoppelt sind, bilden offenbar eine invariante Untergruppe $\mathfrak{U}$ von $\mathfrak{G}_f$. Analog sei $\mathfrak{V}$ die invariante Untergruppe von $\mathfrak{G}_g$, die aus den Elementen besteht, die an E von $\mathfrak{G}_f$ gekoppelt sind. $\mathfrak{U}$ habe die Ordnung u und $\mathfrak{V}$ die Ordnung v. $\mathfrak{U}\cdot\mathfrak{V}$ ist dann eine invariante Untergruppe von $\mathfrak{G}_h$ mit der Ordnung $u\cdot v$. Besteht das vollständige rechtsseitige Restsystem mod $\mathfrak{U}\cdot\mathfrak{V}$ aus k Permutationen $S_{\mu_\varrho}\cdot T_{\mu_\varrho}$, so sind die $u\cdot k$ Permutationen $\mathfrak{U}\cdot S_{\mu_\varrho}$ $(\varrho=1, 2, \ldots, k)$ sämtlich voneinander verschieden wegen der Eigenschaften des Restsystemes und stellen alle Permutationen von $\mathfrak{G}_f$ dar. Analoges gilt für die Permutationen $\mathfrak{V}\cdot T_{\mu_\varrho}$. Also ist $u\cdot k=p\cdot m$ und $v\cdot k=p-1$. Dann folgt $p \mid u$. Nach dem Sylowschen Satze gibt es dann eine Permutation der Ordnung p in $\mathfrak{U}$. Diese Permutation ist an E in $\mathfrak{G}_g$ geknüpft. Nach dem Frobeniusschen Satze gibt es dann unendlich viele Primzahlmoduln q, so daß $h(x)\equiv f(x)\cdot l_1(x)\cdots l_{p-1}(x) \pmod q$ ist und $f(x)$, $l_\nu(x)$ Primfunktionen der bzgl. Grade p und 1 sind. $g(x)$ zerfällt aber nur für Primzahlen der Form $px+1$ in Primfaktoren ersten Grades; also ist q von der Form $px+1$. Somit gibt es nach Dedekind unendlich viele Primzahlen der Form $px+1$, die in dem durch $f(x)=0$ erzeugten Körper $\mathsf{P}(\vartheta)$ Primideale des Grades p sind.

Bemerkung: Unser Satz ist ein Gegenstück zu dem Bauerschen Satz, daß es in jedem endlichen algebraischen Körper des Grades n unendlich viele Primzahlen der Form $nx+1$ gibt, die daselbst in lauter Primideale ersten Grades zerfallen. — Bei uns muß n notwendigerweise eine Primzahl sein, falls man den Satz in so allgemeiner Form aussprechen will, wie der Beweis zeigt. Gegenbeispiel: $x^4+1=0$ besitzt die Vierergruppe als Galoissche Permutationsgruppe, hat also kein Primideal 4. Grades in dem durch $x^4+1=0$ erzeugten Körper $\mathsf{P}(\vartheta)$.

Verallgemeinerung des Satzes: *In jedem algebraischen Zahlkörper* $\mathsf{P}(\vartheta)$ *über* P *vom Grade* n *gibt es unendlich viele Primzahlen der Form* $p\,x+1$, *die in* $\mathsf{P}(\vartheta)$ *mindestens ein Primideal* q*-ten Grades enthalten, wobei* q *eine in* n *aufgehende Primzahl bedeutet, die zu der beliebig vorgegebenen Primzahl* p *in dem Verhältnis steht, daß* q *zu* $p-1$ *teilerfremd ist.*

Beweis: $f(x)=0$ sei die algebraische Gleichung n-ten Grades über P und daselbst irreduzibel, die $\mathsf{P}(\vartheta)$ erzeugt; $g(x)$ sei dasselbe Polynom wie oben. $\mathfrak{G}_f$ ist dann von der Ordnung $n\cdot m$. Es bestehen ferner wie oben die Relationen $u\cdot k=n\cdot m$ und $v\cdot k=p-1$. Wegen $q\,|\,n$ und $(q,\,p-1)=1$ folgt, daß $q\,|\,u$. Nach dem Sylowschen Satze gibt es also in $\mathfrak{U}$ eine Permutation der Ordnung p. Es gibt dann unendlich viele Primzahlmoduln s, so daß

$$h(x)=f(x)\cdot g(x)\equiv\prod_{\nu=1}^{\alpha}P_\nu(x)\cdot\prod_{\nu=1}^{\beta}l_\nu(x)\pmod s,$$

wobei die $P_\nu(x)$ Primfunktionen von den Graden q oder 1 sind, aber mindestens eine den Grad q besitzt. Die $l_\nu(x)$ sind Primfunktionen 1. Grades. Wie oben schließt man dann die obige Verallgemeinerung des Satzes.

Eingegangen 7. Januar 1932.

Formale Theorie der linearen Differentialgleichungen.

(Zweiter Teil).

Von *Oystein Ore* in New Haven (Conn.) U. S. A.

Einleitung.

Im ersten Teil dieser Untersuchungen sind die Hauptresultate der formalen Theorie der linearen Differentialpolynome in abstrakten Differentialkörpern dargestellt worden. Wie man leicht sieht, beruht diese Theorie hauptsächlich auf den Eigenschaften der linearen Gleichungen

$$X(y) \times A(y) + Y(y) \times B(y) = C(y).$$

In diesem zweiten Teil studiere ich eine Reihe von neuen Problemen, die mit den Eigenschaften der *gemischten* Gleichungen

$$A(y) \times X(y) + Y(y) \times B(y) = C(y) \tag{I}$$

eng verbunden sind. Diese Gleichungen (I) sind meines Wissens früher noch nicht in dieser Theorie behandelt worden, aber wie man aus dem folgenden ersehen wird, sind ihre Eigenschaften sowohl hier als auch in einer allgemeineren, nicht-kommutativen Polynomtheorie besonders wichtig.

In § 1 wird die allgemeine Bedingung für die Lösbarkeit einer gemischten Gleichung aufgestellt, und die Lösung auf die spezielle Kongruenz

$$A(y) \times X(y) \equiv 0 \pmod{B(y)} \tag{II}$$

zurückgeführt. In § 2 folgt dann der Hauptsatz der Theorie, daß die Lösungen einer Kongruenz (II) einen endlichen Modul (mod $B(y)$) in bezug auf den Konstantenkörper bilden. Dieser Satz ist analog, aber tieferliegend als der gewöhnliche Hauptsatz über die Integrale linearer Differentialgleichungen; unter den interessantesten Unterschieden ist die Tatsache, daß der Rang des Lösungsmoduls von (II) sehr wohl den Grad n von $A(y)$ übersteigen kann.

In § 3 wird eine Verallgemeinerung des Transformationsbegriffs aus Teil I vorgenommen, und die wichtigsten Eigenschaften der allgemeineren Transformation abgeleitet. Es entsteht sofort die Frage nach denjenigen Polynomen welche ein gegebenes Polynom $A(y)$ in sich selbst oder in einen Teiler transformieren. Ein solches Polynom heißt eine *Eigenwurzel* von $A(y)$, und es folgt aus dem Hauptsatz, daß die Eigenwurzeln einen Ring, den *Eigenring* E von $A(y)$ bilden, und zwar ist der Eigenring ein endliches, hyperkomplexes System in bezug auf den Konstantenkörper. Dies scheint mir eines der wichtigsten Resultate dieser Theorie. Unter den weiteren Eigenschaften von E erwähne ich, daß die Restklassen mod $A(y)$ einen Modul bilden, worin aber im allgemeinen keine Multiplikation möglich ist; der Eigenring besteht genau aus denjenigen Restklassen, für die eine Multiplikation gestattet ist. Zuletzt werden in § 5 verschiedene Anwendungen dieser Theorie gemacht.

In Kap. II wird die Struktur der Differentialpolynome untersucht; durch die Anwendung der Transformation wird diese Untersuchung besonders erleichtert. Die bekannten Resultate von Loewy [1]) über vollreduzible Zerlegungen werden für linke

[1]) A. Loewy: „Über vollständig reduzible lineare homogene Differentialgleichungen", Math. Ann. **62** (1906),

und rechte Darstellungen in symmetrischer Weise ohne Anwendung der adjungierten Polynome abgeleitet; ich füge auch verschiedene neue Sätze hinzu, z. B. die Sätze 3, 4, 8 und 9. In § 3 gebe ich einen neuen Beweis für den zuerst von Krull [2]) bewiesenen Hauptsatz über die Darstellung von Polynomen als Hülle von unzerlegbaren Polynomen. Dieser Beweis ist sehr kurz und übersichtlich, und die sogenannten Zurückleitungsgruppen von Krull konnten gänzlich vermieden werden. Es ist auch von Interesse zu bemerken, daß dieselbe Methode einen kurzen Beweis für den Wedderburnschen Satz über die Zerlegung endlicher Gruppen ergibt. Zuletzt beweise ich, über Krull hinaus, die Ersetzbarkeit der Komponenten zweier Zerlegungen, und daß alle verschiedenen Darstellungen durch Transformation mit Eigenwurzeln erhalten werden können.

Ich mache hier darauf aufmerksam, daß man die Zerlegungssätze von Kap. II auch durch Anwendung der verallgemeinerten Abelschen Gruppen von Krull [3]) hätte ableiten können. Man müßte dann den Restklassenmodul für ein Differentialpolynom als verallgemeinerte Abelsche Gruppe mit dem Ring aller Differentialpolynome als Operatorenbereich auffassen und darauf die Krullschen Sätze anwenden. Ich habe es aber hier bevorzugt, direkte Beweise zu geben.

Um diese Theorie zu vollenden, bleibt nun noch übrig, die Struktur des Eigenringes zu studieren; dies kann im wesentlichen mit den gewöhnlichen Methoden der hyperkomplexen Algebra geschehen, und ich hoffe, in einem letzten Teil diesen Gegenstand zu behandeln. Ich möchte zum Schluß wieder darauf aufmerksam machen, daß dieselbe Theorie für Differenzenpolynome und auch für nicht-kommutative Polynomtheorie anwendbar ist.

Kap. 1. Der Fundamentalsatz.

1. Gemischte Gleichungen.

Im ersten Teil sind hauptsächlich die Gleichungen

$$X(y) \times A(y) + Y(y) \times B(y) = C(y) \tag{1}$$

und

$$A(y) \times X_1(y) + B(y) \times Y_1(y) = C(y) \tag{2}$$

studiert worden, in denen die unbekannten $X(y)$, $Y(y)$ und $X_1(y)$, $Y_1(y)$ entweder beide als linke oder beide als rechte Multiplikatoren vorkommen, und die meisten Resultate in Teil I sind einfache Folgerungen der Untersuchungen über solche Gleichungen (1) und (2).

Es liegt nun nahe, auch *gemischte lineare Gleichungen* von der Form

$$A(y) \times X(y) + Y(y) \times B(y) = C(y) \tag{3}$$

zu studieren, worin die unbekannten Polynome $X(y)$ und $Y(y)$ auf *verschiedenen* Seiten, der bekannten Koeffizienten $A(y)$ und $B(y)$ auftreten. Die Lösung einer Gleichung (3) ist natürlich mit der Lösung der Kongruenz

$$A(y) \times X(y) \equiv C(y) \pmod{B(y)} \tag{4}$$

äquivalent, und wir wollen meistens diese Kongruenzform benutzen.

Wenn der Modul $B(y)$ in (4) vom Grade m ist, so kann man voraussetzen, daß der Grad einer Lösung $X(y)$ höchstens gleich $m - 1$ ist; weiter kann man $A(y)$ als primär voraussetzen.

Wenn nun in (4) $D(y)$ der Durchschnitt von $B(y)$ und $C(y)$ ist, so folgt sofort

---

S. 89—117. „Über lineare homogene Differentialgleichungen derselben Art", Math. Ann. **70** (1911), S. 550—560. „Über die Zerlegung eines linearen homogenen Differentialausdruckes in größte vollständig reduzible Faktoren", Sitzungsber. der Heidelberger Akad. Jahrg. 1917, 8. Abh. Zu erwähnen ist auch die Dissertation von H. Blumberg: „Über algebraische Eigenschaften von linearen homogenen Differentialausdrücken", Göttingen 1912.

[2]) W. Krull: „Über verallgemeinerte endliche Abelsche Gruppen", Math. Zeitschr. **23** (1925), S. 161—196.

[3]) W. Krull: „Theorie und Anwendung der verallgemeinerten Abelschen Gruppen", Sitzungsber. d. Heidelberger Akad. 1926, 1 Abb. Vgl. auch E. Noether u. W. Schmeidler: „Moduln in nicht-kommutativen Bereichen, insbesondere aus Differential- und Differenzenausdrücken", Math. Zeitschr. **8** (1920), S. 1—35.

(5) $$A(y) \times X(y) \equiv 0 \pmod{D(y)}.$$

Im nächsten Paragraphen wollen wir die Lösungen dieser speziellen Kongruenzen mehr eingehend behandeln. Hier genügt es zu bemerken, daß jede Lösung $X(y)$ mod $D(y)$ jedenfalls kongruent einer Lösung $X_0(y)$ derselben Kongruenz ist, wo der Grad von $X_0(y)$ kleiner als der Grad von $D(y)$ ist. Setzt man daher

$$A(y) \times X_0(y) = E(y) \times D(y)$$
$$X(y) = X_0(y) + K(y) \times D(y),$$

in (4) ein, so kann man durch $D(y)$ dividieren und man erhält eine neue Kongruenz von der Form

$$A(y) \times K(y) \equiv C_1(y) \pmod{B_1(y)},$$

wo $B(y) = B_1(y) \times D(y)$ und $C_1(y)$ ein leicht bestimmbares Polynom ist. Setzt man diese Reduktion fort, so erhält man also:

Die Lösung einer Kongruenz (4) *kann auf die Lösung von Kongruenzen* (5) *und Kongruenzen* (4) *zurückgeführt werden, wo* $C(y)$ *zum Modul* $B(y)$ *relativ prim ist.*

Im Fall, wo $C(y)$ zu $B(y)$ relativ prim ist, kann man aber ein notwendiges und hinreichendes Kriterium für die Lösbarkeit aufstellen. Wir brauchen dafür den folgenden Hilfssatz, der auch in anderen Verbindungen von Nutzen ist:

Satz 1. *Aus einer Kongruenz*

(6) $$X(y) \times A(y) \equiv C(y) \pmod{B(y)}$$

folgt

(7) $$CA(y)C^{-1} \times X(y) \equiv AC(y)A^{-1} \pmod{AB(y)A^{-1}}.$$

Da wir hier denselben speziellen Artbegriff wie in Teil I anwenden, muß man natürlich $A(y)$ zu $B(y)$ und $C(y)$ relativ prim voraussetzen; benutzt man aber die allgemeine Transformation von § 3, so gilt der Satz 1 bedingungslos.

Um den Satz zu beweisen, multiplizieren wir (6) links mit $CA(y)C^{-1}$ und erhalten

(8) $$CA(y)\,C^{-1} \times X(y) \times A(y) \equiv a_0\, c_0\, [A(y), C(y)] \pmod{B(y)},$$

wo a_0 und c_0 die höchsten Koeffizienten von $A(y)$ und $C(y)$ sind. Man kann diese Kongruenz (8) auch als

$$(CA(y)\,C^{-1} \times X(y) - AC(y)\,A^{-1}) \times A(y) \equiv 0 \pmod{B(y)}$$

schreiben, woraus (7) nach Satz 5, Teil I folgt.

Für den Spezialfall $C(y) = y$ erhält man das folgende

Korollar. *Wenn*

(9) $$K(y) \times L(y) \equiv y \pmod{M(y)},$$

so ist

(10) $$L(y) \times K(y) \equiv y \pmod{LM(y)\,L^{-1}}.$$

Wir können dann beweisen

Satz 2. *Eine Kongruenz*

(11) $$A(y) \times X(y) \equiv C(y) \pmod{B(y)}, \quad (B(y), C(y)) = y,$$

ist dann und nur dann lösbar, wenn $CB(y)\,C^{-1}$ *mit* $A(y)$ *umstellbar ist.*

Es soll zunächst an die Definition der *Umstellbarkeit* erinnert werden (vgl. § 5, Teil I). Ein Polynom $K(y)$ heißt mit $L(y)$ *umstellbar*, wenn $K(y)$ in der Form $K(y) = LK_1(y)\,L^{-1}$ darstellbar ist, oder, was dasselbe bedeutet, wenn das Produkt

$$K(y) \times L(y) = k_0\, l_0\, [K_1(y), L(y)] = K_1\, L(y)\, K_1^{-1} \times K_1(y)$$

als eine Hülle von $L(y)$ und einem mit $K(y)$ gleichartigen Polynom $K_1(y)$ aufgefaßt werden kann.

Es ist daher $CB(y)\,C^{-1}$ mit $A(y)$ umstellbar, wenn man ein $B_1(y)$ so bestimmen kann, daß

$$CB(y)\,C^{-1} = AB_1(y)\,A^{-1}. \tag{12}$$

Wenn aber (11) eine Lösung hat, so ist

$$CB(y)\,C^{-1} = A(XB(y)\,X^{-1})\,A^{-1},$$

und der zweite Teil des Satzes ist bewiesen. Wenn umgekehrt eine Darstellung (12) besteht, so können wir ein $X_0(y)$ so bestimmen, daß

$$X_0(y) \times A(y) \equiv y \pmod{B_1(y)}$$

und folglich nach dem obenstehenden Korollar

$$A(y) \times X_0(y) \equiv y \pmod{AB_1(y)\,A^{-1}}.$$

Wenn man diese Kongruenz rechts mit $C(y)$ multipliziert und (12) beachtet, so folgt, daß $X_0(y) \times C(y)$ eine Lösung von (11) ist.

Wir erwähnen speziell das

Korollar. *Eine Kongruenz*

$$A(y) \times X(y) \equiv y \pmod{B(y)}$$

ist dann und nur dann lösbar, wenn $B(y)$ mit $A(y)$ umstellbar ist.

Wir kehren nun zu der allgemeinsten Kongruenz (4) zurück. Wenn eine spezielle Lösung $X_0(y)$ schon bekannt ist, so reduziert sich die Bestimmung der allgemeinen Lösung auf die Kongruenz

$$A(y)\,(X(y) - X_0(y)) \equiv 0 \pmod{B(y)},$$

also auf den Spezialfall

$$A(y) \times X(y) \equiv 0 \pmod{B(y)}, \tag{13}$$

den wir im folgenden genauer studieren werden.

2. Beweis des Fundamentalsatzes.

Es ist zunächst klar, daß eventuelle Lösungen von (13) die beiden folgenden Eigenschaften haben: 1. Wenn $X(y)$ eine Lösung bezeichnet, so ist auch $k^{(0)}X(y)$ eine Lösung, wenn $k^{(0)}$ ein beliebiges Element des Konstantenkörpers bezeichnet. 2. Wenn $X_0(y)$ und $X_1(y)$ zwei Lösungen sind, so ist auch $X_0(y) + X_1(y)$ eine Lösung. Die Lösungen bilden daher einen Modul mit dem Konstantenkörper als Multiplikatorenbereich.

Wir wollen aber noch den schärferen Satz beweisen, den wir im folgenden als den *Fundamentalsatz über Kongruenzen* bezeichnen werden:

Satz 3. *Die Lösungen der Kongruenz*

$$A(y) \times X(y) \equiv 0 \pmod{B(y)} \tag{14}$$

bilden einen endlichen Modul mit dem Konstantenkörper als Multiplikatorenbereich, d. h. man kann für die Lösungen $X(y)$ ein solches Fundamentalsystem

$$X_1(y), \ldots, X_r(y)$$

bestimmen, daß eine beliebige Lösung $X(y)$ in der Form

$$X(y) \equiv k_1^{(0)}X_1(y) + \cdots + k_r^{(0)}X_r(y) \pmod{B(y)}$$

darstellbar ist, wo die Koeffizienten Elemente des Konstantenkörpers sind; der Rang r des Moduls ist kleiner als eine nur von den Graden n und m von $A(y)$ und $B(y)$ abhängige Schranke $N(n, m)$.

Ich bemerke hier, daß es beim Beweis dieses Satzes zum ersten Mal notwendig ist, die spezielle Form der Differentialpolynome in Betracht zu ziehen; alles was bis jetzt und im Teil I bewiesen ist, gilt ohne weiteres für beliebige nicht-kommutative Ringe mit Euklidschem Algorithmus.

Wir setzen nach (14)

$$A(y) \times X(y) = Y(y) \times B(y), \tag{15}$$

wo die bekannten Polynome $A(y)$ und $B(y)$ die Form

$$A(y) = y^{(n)} + a_1 y^{(n-1)} + \cdots + a_n y$$
$$B(y) = b_0 y^{(m)} + b_1 y^{(m-1)} + \cdots + b_m y$$

haben, während

$$X(y) = s_0 y^{(m-1)} + s_1 y^{(m-2)} + \cdots + s_{m-1} y$$
$$Y(y) = t_0 y^{(n-1)} + t_1 y^{(n-2)} + \cdots + t_{n-1} y$$

ist, wo die Koeffizienten s_i und t_i Unbekannte sind, die im folgenden zu bestimmen sind.

Wir bilden zunächst die Produkte $A(y) \times X(y)$ und $Y(y) \times B(y)$, und es ist dabei bequem gewisse Abkürzungen einzuführen. Für ein beliebiges $k \geqq 0$ wird

$$y^{(k)} \times X(y) = S_{k,0} y^{(k+m-1)} + S_{k,1} y^{(k+m-2)} + \cdots + S_{k,k+m-1} y \tag{16}$$

gesetzt, wo

$$S_{k,i} = \binom{k}{i} s_0^{(i)} + \binom{k}{i-1} s_1^{(i-1)} + \cdots = \sum_{j=0}^{i} \binom{k}{i-j} s_j^{(i-j)}. \tag{17}$$

Speziell ist für alle k

$$S_{k,0} = s_0, \tag{18}$$

und für $i \geqq k$, etwa $i = k + r$, nimmt $S_{k,i}$ die Form

$$S_{k,k+r} = s_r^{(k)} + \binom{k}{1} s_r^{(k-1)} + \cdots \tag{19}$$

an. Aus (16) erhält man sofort

$$A(y) \times X(y) = S_{n,0} y^{(n+m-1)} + (S_{n,1} + a_1 S_{n-1,0}) y^{(n+m-2)} + (S_{n,2} + a_1 S_{n-1,1} + a_2 S_{n-2,0}) y^{(n+m-3)} + \cdots \tag{20}$$

und in derselben Weise

$$Y(y) \times B(y) = t_0 B_{n-1,0} y^{(n+m-1)} + (t_0 B_{n-1,1} + t_1 B_{n-2,0}) y^{(n+m-2)} + \cdots, \tag{21}$$

wo wie in (17)

$$B_{k,i} = \sum_{j=0}^{i} \binom{k}{i-j} b_j^{(i-j)} \tag{22}$$

gesetzt worden ist; die $B_{k,i}$ können daher als bekannte Größen betrachtet werden.

Wir setzen nun (20) und (21) in (15) ein und vergleichen die Koeffizienten beider Seiten. Man erhält dadurch das folgende System von Gleichungen, das wir hier studieren werden:

$$\begin{cases}
(n) & S_{n,0} = t_0 B_{n-1,0} \\
 & S_{n,1} + a_1 S_{n-1,0} = t_0 B_{n-1,1} + t_1 B_{n-2,0} \\
 & S_{n,2} + a_1 S_{n-1,1} + a_2 S_{n-2,0} = t_0 B_{n-1,2} + t_1 B_{n-2,1} + t_2 B_{n-3,0} \\
 & \cdots\cdots\cdots\

wie bemerkt $j \leqq n-1$ ist, kommen in der Darstellung von t_k keine höheren als die $(n-1)$-ten Derivierten der s_k vor, so daß die Darstellung in der Form

$$t_k = \sum_{i,j=0}^{m-1,n-1} D_{k,i,j}\, s_i^{(j)} \qquad (k = 0, 1, \ldots, n-1) \tag{25}$$

erscheinen wird, wobei die $D_{k,i,j}$ wieder bekannte Größen aus K sind.

Wir substituieren nun (25) rechts in die übrigbleibenden m Gleichungen (23); die rechte Seite einer jeden solchen Gleichung wird dann wieder von der Form (25). Dasselbe gilt auch für die rechte Seite wenn man die $S_{i,j}$ durch ihre Ausdrücke (17) ersetzt; eine Ausnahme bilden nur die Glieder

$$S_{n,n},\ S_{n,n+1},\ \ldots,\ S_{n,n+m-1},$$

indem jedes $S_{n,n+r}$ nach (19) ein Glied $s_r^{(n)}$ enthält. Da jede Gleichung nur ein einziges solches Glied enthält, so erhält man

$$s_r^{(n)} = \sum_{i,j=0}^{m-1,n-1} E_{r,i,j}\, s_i^{(j)} \qquad (r = 0, 1, \ldots, m-1). \tag{26}$$

Wir derivieren nun beide Seiten von (26) für ein bestimmtes r. Rechts werden dann auch Glieder vorkommen, welche n-te Derivierte der s_i enthalten; diese $s_i^{(n)}$ kann man aber durch die Ausdrücke (26) ersetzen, wodurch man auch für $s_r^{(n+1)}$ eine Darstellung von der Form (16) erhält. Indem man diese Schlüsse wiederholt, zeigt man:

Für eine beliebige Derivierte eines Koeffizienten s_r in $X(y)$ besteht eine Darstellung

$$s_r^{(k)} = \sum_{i,j=0}^{m-1,n-1} F_{r,k,i,j}\, s_i^{(j)} \qquad (r = 0, 1, \ldots, m-1,\ k = 0, 1, \ldots), \tag{27}$$

wobei die Koeffizienten $F_{r,k,i,j}$ aus den Koeffizienten von $A(y)$ und $B(y)$ und ihren Derivierten rational in K bestimmbar sind.

Es ist selbstverständlich, daß dies auch für die bis jetzt ausgeschlossenen Werte

$$k = 0, 1, \ldots, n-1 \quad \text{gilt.}$$

Nach (27) sind alle $s_r^{(k)}$ $(k = 0, 1, \ldots)$ für ein gegebenes r linear durch die nm Größen

$$s_i^{(j)} \qquad (i = 0, 1, \ldots, m-1,\ j = 0, 1, \ldots, n-1)$$

ausdrückbar, und je $nm+1$ unter den $s_r^{(k)}$ $(k = 0, 1, \ldots)$ müssen daher in K linear abhängig sein, daher:

Jeder Koeffizient s_r von $X(y)$ muß einer linearen homogenen Differentialgleichung

$$y^{(n_r)} + K_{1,r}\, y^{(n_r-1)} + \cdots + K_{n_r,r} = 0 \tag{28}$$

genügen, worin $n_r \leqq nm$, und wo die Koeffizienten K rational von den Koeffizienten von $A(y)$ und $B(y)$ und ihren Derivierten abhängen.

Wir betrachten nun alle Lösungen $X(y)$ von (15) vom Grade $\leqq m-1$; die Koeffizienten s_r eines bestimmten $y^{(m-1-r)}$ in solchen Lösungen $X(y)$ genügen dann alle (28). Setzt man aber n_r+1 solche Koeffizienten s_r in (28) ein, erhält man ein lineares System in den Koeffizienten $K_{i,r}$, und die entsprechende Wronskische Determinante $\triangle(s_{r,1} \ldots s_{r,n_r+1})$ muß folglich verschwinden. Nach einem schon in § 1, Teil I, erwähnten Satz folgt aber dann, daß das System der Koeffizienten s_r in bezug auf den Konstantenkörper eine endliche Basis vom Range $\leqq n_r$ besitzt.

Der Beweis des Fundamentalsatzes läßt sich nun einfach vollenden. Es sei nämlich

$$s_{0,1},\ s_{0,2},\ \ldots,\ s_{0,m_0},\ m_0 \leqq n_0 \leqq nm, \tag{29}$$

eine Basis für das System der höchsten Koeffizienten s_0, so daß ein beliebiger Koeffizient s_0 in der Form

$$s_0 = k_{0,1}\, s_{0,1} + \cdots + k_{0,m_0}\, s_{0,m_0} \tag{30}$$

darstellbar ist, wo alle $k_{0,i}$ im Konstantenkörper liegen. Weiter seien

$$X_{0,1}(y), \ldots, X_{0,m_0}(y)$$

diejenigen Lösungen von (15), welche die höchsten Koeffizienten (29) haben. Wenn dann die beliebige Lösung $X(y)$ den höchsten Koeffizient s_0 hat, so wird nach (30)

$$X(y) = k_{0,1} X_{0,1}(y) + \cdots + k_{0,m_0} X_{0,m_0}(y) + X_1(y),$$

wo $X_1(y)$ eine Lösung mit $s_0 = 0$ ist. Wie früher finden wir, daß die Koeffizienten aller Lösungen mit $s_0 = 0$ auch endliche Basen in bezug auf den Konstantenkörper haben, und es wird in derselben Weise

$$X_1(y) = k_{1,1} X_{1,1}(y) + \cdots + k_{1,m_1} X_{1,m_1}(y) + X_2(y),$$

wo in $X_2(y)$ $s_0 = s_1 = 0$. In dieser Weise folgt dann zuletzt die Existenz eines Fundamentalsystems und auch die Behauptung über die Anzahl r der Glieder eines solchen Systems.

3. Allgemeine Transformation.

In 4, Teil I, haben wir die Transformation eines Polynoms $A(y)$ durch ein zweites $B(y)$ durch die Formel

$$BA(y)\,B^{-1} = a_0\,b_0\,[A(y), B(y)] \times B(y)^{-1} \tag{31}$$

definiert, wobei a_0 und b_0 bzw. die höchsten Koeffizienten dieser Polynome sind. Diese Definition wollen wir jetzt für beliebige Polynome $A(y)$ und $B(y)$ gelten lassen, während wir in Teil I nur den Fall studiert haben, wo $A(y)$ zu $B(y)$ relativ prim ist, und $BA(y)\,B^{-1}$ daher vom selben Grade wie $A(y)$ ist. Man erhält entsprechend einen allgemeineren Artbegriff, indem wir allgemein sagen, daß $BA(y)\,B^{-1}$ mit $A(y)$ gleichartig ist. Man muß aber dabei bemerken, daß der allgemeinere Artbegriff nicht symmetrisch ist, indem $BA(y)\,B^{-1}$ vom Grade $n - d$ wird, wenn $A(y)$ den Grad n und $D(y) = (A(y), B(y))$ den Grad d hat.

Die allgemeine Transformation läßt sich sofort auf die spezielle zurückführen. Wenn nämlich

$$A(y) = A_1(y) \times D(y), \quad B(y) = B_1(y) \times D(y), \tag{32}$$

so folgt nach (31)

$$BA(y)\,B^{-1} = B_1\,A_1(y)\,B_1^{-1}, \tag{33}$$

und dies gilt allgemeiner für einen beliebigen gemeinsamen Teiler $D(y)$ von $A(y)$ und $B(y)$.

Wenn speziell $D(y)$ ein *primärer Teiler* von $A(y)$ ist, also etwa $A(y) = A_1(y) \times D(y)$, so wird

$$DA(y)\,D^{-1} = A_1(y), \tag{34}$$

d. h. *jeder linksseitige Faktor $A_1(y)$ von $A(y)$ mit dem höchsten Koeffizienten a_0 ist mit $A(y)$ gleichartig.* Noch spezieller folgt

$$AA(y)\,A^{-1} = a_0\,y.$$

Im folgenden werden wir die wichtigsten Eigenschaften der allgemeinen Transformation ableiten; in manchen Beziehungen stimmen sie mit den früher für spezielle Transformation bewiesenen Eigenschaften überein.

Zuerst beweisen wir

Satz 4. *Wenn $B(y) \equiv \bar{B}(y) \pmod{A(y)}$, so ist*

$$BA(y)\,B^{-1} = \bar{B}A(y)\,\bar{B}^{-1}$$

$B(y)$ und $\bar{B}(y)$ müssen nämlich denselben Durchschnitt $D(y)$ mit $A(y)$ haben, und nach Division mit $D(y)$ erhält man $B_1(y) \equiv \bar{B}_1(y) \pmod{A_1(y)}$, und der Satz folgt aus (33) und Satz 4, Teil I.

Für spezielle Transformation hatten wir weiter den wichtigen Satz: Wenn $A(y)\,B(y)$ durch $C(y)$ teilbar und $B(y)$ zu $C(y)$ relativ prim ist, so muß $A(y)$ durch $BC(y)\,B^{-1}$ teilbar sein. Für allgemeine Transformation lautet der Satz einfacher:

Satz 5. *Wenn ein Produkt $A(y) \times B(y)$ durch $C(y)$ teilbar ist, so wird $A(y)$ durch $BC(y)\,B^{-1}$ teilbar.*

Wenn nämlich

$$B(y) = B_1(y) \times D(y), \qquad C(y) = C_1(y) \times D(y), \qquad (B_1(y), C_1(y)) = y$$

ist, so muß $A(y) \times B_1(y)$ durch $C_1(y)$ teilbar, also $A(y)$ durch $B_1\,C_1(y)\,B_1^{-1}$ teilbar sein, w. z. b. w.

Die Identität

$$(CB)\,A(y)\,(CB)^{-1} = C(BA(y)\,B)\,C \tag{35}$$

bleibt auch für allgemeine Transformation richtig, wie man leicht sieht, wenn man beide Seiten von (35) rechts mit $C(y) \times B(y)$ multipliziert.

Aus (35) folgt die Transivität des allgemeinen Artbegriffes; wie wir schon gesehen haben, ist er aber nicht symmetrisch. Der Satz 7, Teil I, kann aber durch den folgenden ersetzt werden:

Satz 6. *Wenn $\bar{A}(y) = BA(y)\,B^{-1}$, so ist $A(y)$ im speziellen Sinn mit einem linken Teiler $A_1(y)$ von $A(y)$ gleichartig.*

Dies ist eine Folgerung aus (33). Für die Transformation eines Produkts erhält man wie früher die Formel

$$C(B(y) \times A(y))\,C^{-1} = C_1\,B(y)\,C_1^{-1} \times CA(y)\,C^{-1}, \tag{36}$$

wo

$$C_1(y) = AC(y)\,A^{-1}. \tag{37}$$

Setzt man nämlich

$$a_0\,b_0\,c_0\,[B(y) \times A(y),\ C(y)] = K(y) \times a_0\,c_0\,[A(y),\ C(y)], \tag{38}$$

so erhält man nach Division mit $A(y)$

$$b_0\,c_0\,[B(y),\ AC(y)\,A^{-1}] = K(y) \times AC(y)\,A^{-1},$$

woraus wieder $K(y) = C_1\,B(y)\,C_1^{-1}$. Setzt man diesen Wert in (38) ein und dividiert durch $C(y)$, so erhält man (36). Für die Transformation einer beliebigen Anzahl von Faktoren besteht eine entsprechende Formel. Aus (36) folgt

Satz 7. *Wenn $T(y)$ ein Teiler von $A(y)$ ist, so ist $BT(y)\,B^{-1}$ ein Teiler von $BA(y)\,B^{-1}$.*

Etwas schwerer zu beweisen ist die Umkehrung:

Satz 8. *Jeder Teiler von $BA(y)\,B^{-1}$ hat die Form $BT(y)\,B^{-1}$, wo $T(y)$ ein Teiler von $A(y)$ ist.*

Wir nehmen zunächst $B(y)$ zu $A(y)$ relativ prim an, und es sei $T_1(y)$ ein Teiler von $BA(y)\,B^{-1}$, also

$$BA(y)\,B^{-1} = K(y) \times T_1(y). \tag{39}$$

Wir bestimmen ein $B_1(y)$, so daß

$$B_1(y) \times B(y) \equiv y \pmod{A(y)}, \tag{40}$$

und transformieren beide Seiten von (39) durch $B_1(y)$. Man erhält dann nach (36)

$$A(y) = K_1(y) \times B_1\,T_1(y)\,B_1^{-1},$$

und folglich ist

$$T(y) = B_1\,T_1(y)\,B^{-1}$$

ein Teiler von $A(y)$; transformiert man weiter $T(y)$ mit $B(y)$, so ergibt sich

$$BT(y)\,B^{-1} = (BB_1)\,T_1(y)\,(BB_1)^{-1}. \tag{41}$$

Aus (40) folgt aber nach Satz 1

$$B(y) \times B_1(y) \equiv y \pmod{BA(y)\,B^{-1}},$$

und da $T_1(y)$ ein Teiler von $BA(y)\,B^{-1}$ ist, besteht diese Kongruenz auch mod $T_1(y)$, und nach (41) ist daher $T_1(y) = BT(y)\,B^{-1}$.

Wenn aber $B(y)$ zu $A(y)$ nicht relativ prim ist, sondern die Form (32) hat, so ist nach (33) und nach dem schon bewiesenen

$$T_1(y) = B_1 \bar{T}(y) B_1^{-1},$$

wo $\bar{T}(y)$ ein Teiler von $A_1(y)$ ist; nach der Definition der allgemeinen Transformation ist aber

$$T_1(y) = B(\bar{T}(y) \times D(y)) B^{-1},$$

und $\bar{T}(y) \times D(y)$ ist ein Teiler von $A(y)$.

Für die Transformation einer Hülle hat man

$$C[A(y), B(y)]C^{-1} = [CA(y)C^{-1}, CB(y)C^{-1}], \tag{42}$$

wofür man leicht den Beweis findet.

Wir wollen zuletzt diese Untersuchungen anwenden um dem Fundamentalsatz eine neue Fassung zu geben. Aus der Kongruenz

$$A(y) \times X(y) \equiv 0 \pmod{B(y)} \tag{43}$$

folgt nach Satz 5

$$A(y) \equiv 0 \pmod{XB(y)X^{-1}}, \tag{44}$$

und aus (44) folgt umgekehrt (43), so daß man nach dem Fundamentalsatz sagen kann:

Satz 9. *Es sei $A(y)$ ein gegebenes Polynom und $XB(y)X^{-1}$ diejenigen Teiler von $A(y)$, welche einem zweiten gegebenen Polynom $B(y)$ im allgemeinen Sinn gleichartig sind. Die Transformatoren $X(y)$ bilden dann* mod $B(y)$ *einen endlichen Modul in bezug auf den Konstantenkörper.*

4. Invariante Transformatoren.

Eine Wurzel der speziellen Kongruenz

$$A(y) \times I(y) \equiv 0 \pmod{A(y)} \tag{45}$$

wollen wir im folgenden eine *Eigenwurzel von $A(y)$* nennen; es ist zunächst klar, daß $I(y) = y$ und auch jedes durch $A(y)$ teilbare Polynom eine Eigenwurzel ist.

Die Eigenwurzeln mod $A(y)$ sind auch durch die folgende Eigenschaft charakterisiert:

Satz 10. *Eine beliebige Kongruenz* mod $A(y)$ *darf sowohl rechts als links mit einer Eigenwurzel von $A(y)$ multipliziert werden.*

Wenn nämlich $I(y)$ der Kongruenz (45) genügt, so folgt aus

$$M(y)_1 \equiv M_2(y) \pmod{A(y)}$$

sicher

$$M_1(y) \times I(y) \equiv M_2(y) \times I(y) \pmod{A(y)},$$

und die Eigenwurzeln sind die einzigen Polynome mit dieser Eigenschaft für eine beliebige Kongruenz, denn dann muß aus der speziellen Kongruenz $A(y) \equiv 0 \pmod{A(y)}$ auch (45) folgen.

Aus (45) schließt man nach Satz 5:

Satz 11. *Ein Polynom $I(y)$ ist dann und nur dann eine Eigenwurzel von $A(y)$, wenn*

$$A(y) \equiv 0 \pmod{IA(y)I^{-1}}. \tag{46}$$

Wenn $I(y)$ zu $A(y)$ relativ prim ist, so folgt aus (46)

$$IA(y)I^{-1} = A(y), \tag{47}$$

d. h. $A(y)$ *wird durch Transformation mit $I(y)$ ungeändert.* Wir wollen daher auch gelegentlich die Eigenwurzeln *invariante Transformatoren* von $A(y)$ nennen.

Man kann nun den Fundamentalsatz auf die spezielle Kongruenz (45) anwenden, und es leuchtet ein, daß die Eigenwurzeln von $A(y)$ einen endlichen Modul in bezug auf

den Konstantenkörper bilden. Aus (45) erhält man aber auch leicht, daß das Produkt von zwei Eigenwurzeln wieder eine Eigenwurzel ist.

Satz 12. *Die Eigenwurzeln eines Polynoms $A(y)$ bilden einen Schiefring E_A der im folgenden der Eigenring von $A(y)$ heißen soll. Der Eigenring* mod $A(y)$ *ist endlich in bezug auf den Konstantenkörper $K^{(0)}$ und der Rang ist kleiner als eine nur vom Grade n von $A(y)$ abhängige Schranke $N(n)$.*

Der Eigenring E_A ist assoziativ und distributiv und hat das Einheitselement $I(y)=y$; unter den weiteren Eigenschaften von E soll erwähnt werden:

Satz 13. *Jede zu $A(y)$ relativ prime Eigenwurzel besitzt eine eindeutige inverse.*

Wenn nämlich $I(y)$ zu $A(y)$ relativ prim ist, so kann man ein mod $A(y)$ eindeutiges $I_1(y)$ so bestimmen, daß

$$I_1(y) \times I(y) \equiv y \pmod{A(y)}, \tag{48}$$

und $I_1(y)$ ist eine Eigenwurzel, wie aus

$$(I_1 I)\, A(y)\, (I_1 I)^{-1} = I_1 A(y) I_1^{-1} = A(y)$$

folgt. Aus (48) folgt weiter, daß

$$I(y) \times I_1(y) \equiv y \pmod{A(y)}, \tag{49}$$

und für ein gegebenes $I(y)$ gibt es nur eine einzige Eigenwurzel $I_1(y)$, welche der Kongruenz (49) genügt, denn dann erhält man aus (49) wieder (48).

Aus Satz 12 kann man einen weiteren wichtigen Schluß ziehen. Wenn nämlich $I(y)$ eine Eigenwurzel von $A(y)$ ist, so hat $I(y) \times I(y) = I^{(2)}(y)$ und allgemeiner jede symbolische Potenz $I^{(r)}(y)$ dieselbe Eigenschaft. Da aber je $N(n)$ von diesen Potenzen mod $A(y)$ in bezug auf $K^{(0)}$ linear abhängig sind, so folgt

Satz 14. *Jedes Element des Eigenringes von $A(y)$ genügt einer Kongruenz*

$$I^{(r)}(y) + k_1 I^{(r-1)}(y) + \cdots + k_{r-1} I(y) + k_r y \equiv 0 \pmod{A(y)}, \tag{50}$$

wo $r < N(n)$ und alle k im Konstantenkörper liegen.

Wir wollen später den Eigenring genauer studieren; um aber seine Bedeutung klarer zu machen, wollen wir hier seine Beziehung zu den Restklassen mod $A(y)$ kurz behandeln.

Wir sagen, daß zwei Polynome $R_1(y)$ und $R_2(y)$ zu derselben *Restklasse* R mod $A(y)$ gehören, wenn

$$R_2(y) \equiv R_2(y) \pmod{A(y)}. \tag{51}$$

Wenn weiter $S_1(y)$ und $S_2(y)$ zwei Elemente einer zweiten Restklasse S sind, also

$$S_1(y) \equiv S_2(y) \pmod{A(y)}, \tag{52}$$

so wird die Restklasse $R \pm S$ eindeutig bestimmt, wenn man festlegt, daß sie das Element $R_1(y) \pm S_1(y)$ enthalten soll, denn aus (51) und (52) folgt

$$R_1(y) \pm S_1(y) \equiv R_2(y) \pm S_2(y) \pmod{A(y)}.$$

Das Produkt von zwei Restklassen läßt sich aber nicht so definieren, denn aus (51) und (52) kann man nur

$$R_1(y) \times S_1(y) \equiv R_2(y) \times S_2(y) + K(y) \times A(y) \times S_1(y) \pmod{A(y)} \tag{53}$$

schließen, wo $K(y)$ ein beliebiges Polynom ist. Das letzte Glied in (53) verschwindet für beliebige $K(y)$ nur dann, wenn

$$A(y) \times S_1(y) \equiv 0 \pmod{A(y)},$$

d. h. wenn $S_1(y)$ eine Eigenwurzel von $A(y)$ ist. Man kann also sagen:

Man kann das Produkt RS aus zwei Restklassen R und S mod $A(y)$ *nur dann bilden, wenn S eine Eigenklasse* mod $A(y)$ *ist.*

Dabei heißt natürlich S eine *Eigenklasse*, wenn ein und somit alle Elemente von S Eigenwurzeln von $A(y)$ sind.

Die Elemente einer beliebigen Restklasse R mod $A(y)$ haben alle den größten gemeinsamen Teiler $D(y)$ mit $A(y)$, und wir wollen $D(y)$ den *Teiler* von R nennen; wenn $D(y) = y$, heißt R eine *Primklasse.* Wenn weiter $C(y)$ ein bestimmtes Polynom ist, so liegen alle Produkte $C(y) \times R(y)$, wo $R(y)$ der Klasse R gehört, in derselben Restklasse die wir mit $C(y) \times R$ bezeichnen.

Wenn man nun alle Produkte $R_1(y) \times S_1(y)$ aus den Elementen der beiden Restklassen R und S mod $A(y)$ bildet, so liegen diese Produkte in verschiedenen Restklassen mod $A(y)$, wenn S keine Eigenklasse ist; wir wollen untersuchen, wie diese Produkte sich auf die verschiedenen Restklassen verteilen.

Es sei $D(y)$ der Teiler der Restklasse $A(y) \times S$; dann folgt aus (53)

$$R_1(y) \times S_1(y) \equiv R_2(y) \times S_2(y) \pmod{D(y)}.$$

Wenn aber diese Bedingung erfüllt ist, so können die Produkte in sonst beliebige Restklassen fallen, denn wenn $T(y)$ ein beliebiges, durch $D(y)$ teilbares Polynom ist, so kann man nach § 2, Teil I, immer ein $K(y)$ so bestimmen, daß

$$K(y) \times A(y) \times S_1(y) \equiv T(y) \pmod{A(y)}.$$

Satz 15. *Es sei $D(y)$ der Teiler der Restklasse $A(y) \times S$ mod $A(y)$; bildet man dann die sämtlichen Produkte $R(y) \times S(y)$ aus den Elementen der Restklassen R und S* mod $A(y)$, *so müssen sie alle derselben Restklasse* mod $D(y)$ *gehören, aber verteilen sich sonst auf beliebige Klassen* mod $A(y)$.

Wenn $A(y) \times S$ eine Primklasse mod $A(y)$ ist, so verteilen sich also die Produkte auf alle Restklassen, und man kann daher, wenn $T(y)$ ein beliebiges Polynom ist, immer solche Elemente $R(y)$ und $S(y)$ in R und S bestimmen, daß

$$R(y) \times S(y) \equiv T(y) \pmod{A(y)}.$$

Es soll zuletzt bemerkt werden, daß man genau so, wie man hier rechtsseitige Eigenwurzeln eingeführt hat, auch linksseitige Eigenwurzeln definieren und alle früher abgeleitete Resultate auf sie übertragen kann.

Aus (45) folgt sofort

$$A(y) \times I(y) = J(y) \times A(y),$$

wo $J(y)$ eine linksseitige Eigenwurzel ist, und es ergibt sich hieraus

Satz 16. *Jede linksseitige Eigenwurzel von $A(y)$ hat die Form*

$$J(y) = A(y) \times I(y) \times A(y)^{-1}, \tag{53}$$

wo $I(y)$ eine rechtsseitige Eigenwurzel, und durch diese Korrespondenz erhält man einen Isomorphismus zwischen dem rechten und linken Eigenring.

5. Anwendungen.

Wir kehren nun zu der allgemeinen Kongruenz

$$M(y) \times X(y) \equiv 0 \pmod{A(y)} \tag{54}$$

zurück; nach dem Fundamentalsatz hat der Modul M der Lösungen $X(y)$ von (54) einen endlichen Rang m in bezug auf den Konstantenkörper $K^{(0)}$. Wenn aber $X_1(y)$ eine Lösung von (54) ist, so hat $X_1(y) \times I(y)$ dieselbe Eigenschaft, wo $I(y)$ alle Eigenwurzeln von $A(y)$ durchläuft; es folgt daher, daß man solche Lösungen

$$X_1(y), \ldots, X_{m_0}(y)$$

von (54) bestimmen kann, daß eine beliebige Lösung eindeutig in der Form

$$X(y) \equiv X_1(y) \times I_1(y) + \cdots + X_{m_0}(y) \times I_{m_0}(y) \pmod{A(y)} \tag{55}$$

darstellbar ist. Wir wollen m die *Anzahl* der Lösungen von (54) nennen, und wenn e_0 der Rang des Eigenringes E_A von $A(y)$ in bezug auf K ist, so folgt

$$m = m_0 e_0. \tag{56}$$

Satz 17. *Die Lösungen von* (54) *bilden einen endlichen Modul M* mod $A(y)$ *in bezug auf den Konstantenkörper, und der Rang von M ist durch den Rang des Eigenringes* E_A *von* $A(y)$ *teilbar. M ist auch als ein Modul mit* E_A *als rechtem Multiplikatorenbereich darstellbar.*

Es sollen nun ein paar weitere Probleme behandelt werden, bei denen die Eigenwurzeln eine Rolle spielen.

Es sei zunächst $\bar{A}(y) = BA(y)B^{-1}$ ein Polynom das (im speziellen Sinn) mit $A(y)$ von derselben Art ist; man kann dann, wenn die Eigenwurzeln $I(y)$ von $A(y)$ bekannt sind, auch einfach die Eigenwurzeln $\bar{I}(y)$ von $\bar{A}(y)$ erhalten. Eine Eigenwurzel $\bar{I}(y)$ ist nach Satz 11 durch

$$BA(y)\,B^{-1} = T(y) \times (\bar{I}B)\,A(y)\,(\bar{I}B)^{-1} \tag{57}$$

charakterisiert; wenn man $B_1(y)$ durch

$$B_1(y) \times B(y) \equiv y \pmod{A(y)} \tag{58}$$

bestimmt, so folgt aus (57) nach der Formel (36)

$$A(y) = T(y) \times (B_1\bar{I}B)\,A(y)\,(B_1\bar{I}B)^{-1},$$

und es muß

$$B_1(y) \times \bar{I}(y) \times B(y) = I(y)$$

eine Eigenwurzel von $A(y)$ sein; nach Multiplikation mit $B(y)$ erhält man

$$B(y) \times B_1(y) \times \bar{I}(y) \times B(y) = B(y) \times I(y). \tag{59}$$

Nach Satz 1 folgt aber aus (58)

$$B(y) \times B_1(y) \equiv y \pmod{BA(y)\,B^{-1}},$$

und da $\bar{I}(y)$ eine Eigenwurzel von $BA(y)\,B^{-1}$ ist,

$$B(y) \times B_1(y) \times \bar{I}(y) \equiv \bar{I}(y) \pmod{BA(y)\,B^{-1}},$$

daraus weiter

$$B(y) \times B_1(y) \times \bar{I}(y) \times B(y) \equiv \bar{I}(y) \times B(y) \pmod{A(y)},$$

und ein Vergleich mit (59) zeigt, daß

$$\bar{I}(y) \times B(y) \equiv B(y) \times I(y) \pmod{A(y)}. \tag{60}$$

Umgekehrt ist jedes Polynom $\bar{I}(y)$, das der Kongruenz (60) genügt, eine Eigenwurzel von $BA(y)B^{-1}$, denn man erhält

$$(\bar{I}B)\,A(y)\,(\bar{I}B)^{-1} = (BI)\,A(y)\,(BI)^{-1},$$

und da $IA(y)I^{-1}$ ein Teiler von $A(y)$ ist, so wird nach Satz 7 $(BI)\,A(y)\,(BI)^{-1}$ ein Teiler von $BA(y)B^{-1}$, w. z. b. w.

Satz 18. *Der Eigenring von* $BA(y)B^{-1}$, $(A(y), B(y)) = y$, *ist mit dem Eigenring von* $A(y)$ *isomorph, und man erhält sämtliche Eigenwurzeln* $\bar{I}(y)$ *von* $BA(y)B^{-1}$ *aus der Kongruenz*

$$\bar{I}(y) \times B(y) \equiv B(y) \times I(y) \pmod{A(y)},$$

wo $I(y)$ *den Eigenring von* $A(y)$ *durchläuft.*

Wenn es sich aber um gleichartige Polynome im allgemeinen Sinn handelt, wenn also $A(y)$ und $B(y)$ einen Durchschnitt $D(y)$ haben und folglich von der Form (32) sind, so geht (57) in

$$BA(y)B^{-1} = B_1\,A_1(y)\,B_1^{-1} = T(y) \times (\bar{I}B)\,A_1(y)\,(\bar{I}B)^{-1}$$

über, und man hat daher diesen Fall auf den speziellen zurückgeführt. Es ist somit nach Satz 18

$$\bar{I}(y) \times B(y) \equiv B_1(y) \times I_1(y) \pmod{A_1(y)},$$

wo $I_1(y)$ zum Eigenring von $A_1(y)$ gehört. Multipliziert man rechts mit $D(y)$, so erhält man für den allgemeinen Fall die Relation

$$\bar{I}(y) \times B(y) \equiv B_1(y) \times I_1(y) \times D(y) \pmod{A(y)}. \tag{61}$$

Man kann weiter fragen, wann eine Identität

$$CA(y)C^{-1} = BA(y)B^{-1} \tag{62}$$

bestehen kann; wir setzen wie früher spezielle Transformation voraus. Wir bestimmen ein $B_1(y)$ aus (58). Wenn man (62) mit $B_1(y)$ transformiert, so ergibt sich

$$(B_1C)\,A(y)\,(B_1C)^{-1} = A(y),$$

und es ist daher $B_1(y) \times C(y) = I(y)$ eine Eigenwurzel von $A(y)$. Multipliziert man diese Gleichung links mit $B(y)$, so erhält man

$$B(y) \times B_1(y) \times C(y) = B(y) \times I(y); \tag{63}$$

andererseits erhält man aus (58) und Satz 1, indem man (62) berücksichtigt,

$$B(y) \times B_1(y) \equiv y \pmod{CA(y)C^{-1}},$$

woraus nach rechter Multiplikation mit $C(y)$

$$B(y) \times B_1(y) \times C(y) \equiv C(y) \pmod{A(y)}$$

folgt. Wenn man dies mit (63) vergleicht, erhält man

Satz 19. *Eine Identität*

$$CA(y)C^{-1} = BA(y)B^{-1}, \quad (B(y),\ A(y)) = y,$$

kann dann und nur dann stattfinden, wenn

$$C(y) \equiv B(y) \times I(y) \pmod{A(y)},$$

wo $I(y)$ eine zu $A(y)$ relativ prime Eigenwurzel von $A(y)$ ist.

Der Fall, wo es sich um gleichartige Polynome im allgemeinen Sinn handelt, ist etwas komplizierter.

Zuletzt wollen wir untersuchen, wann eine Identität

$$AB(y)A^{-1} = AC(y)A^{-1} \tag{64}$$

bestehen kann, wobei wieder spezielle Transformation vorausgesetzt wird. Die Gleichung (64) ist natürlich mit

$$[A(y),\ B(y)] = [A(y),\ C(y)] \tag{65}$$

gleichwertig.

Aus (64) folgt zunächst, daß $C(y)$ mit $B(y)$ von derselben Art ist, so daß man $C(y) = KB(y)K^{-1}$ schreiben kann; setzt man dies in (64) ein, so erhält man

$$AB(y)A^{-1} = (AK)\,B(y)\,(AK)^{-1}$$

und daraus nach Satz 19

$$A(y) \times K(y) \equiv A(y) \times I(y) \pmod{B(y)},$$

wo $I(y)$ eine Eigenwurzel von $B(y)$ ist. Die letzte Kongruenz kann man auch in der Form

$$A(y) \times (K(y) - I(y)) \equiv 0 \pmod{B(y)}$$

schreiben, und man erhält daher zuletzt

$$K(y) \equiv I(y) + R(y) \pmod{B(y)},$$

wo $R(y)$ eine beliebige Wurzel der Kongruenz

$$A(y) \times X(y) \equiv 0 \pmod{B(y)} \tag{66}$$

ist; umgekehrt erhält man aus einem $K(y)$ von dieser Form eine Identität (64).

Satz 20. *Eine Identität*

$$AB(y)A^{-1} = AC(y)A^{-1}, \qquad (A(y),\ B(y)) = y,$$

besteht dann und nur dann, wenn $C(y) = KB(y)K^{-1}$ und das Polynom $K(y)$ die Form

$$K(y) \equiv I(y) + R(y) \pmod{B(y)}$$

hat, wo $I(y)$ eine zu $B(y)$ relativ prime Eigenwurzel von $B(y)$ und $R(y)$ eine Wurzel der Kongruenz (66) *ist.*

Kap. II. Darstellungen der Differentialpolynome.

1. Vollreduzible Polynome.

Es sollen in diesem Kapitel zwei Normaldarstellungen der Differentialpolynome untersucht werden, nämlich die Darstellung als *Produkt von vollreduziblen Faktoren* und die Darstellung als *Hülle von unzerlegbaren Faktoren.* In Teil I haben wir eine dritte Normaldarstellung untersucht, nämlich die Darstellung als Produkt von Primfaktoren.

Die Hauptresultate über vollreduzible Darstellungen stammen von Loewy [4]); im folgenden werden sie in einer neuen Weise abgeleitet, u. a. vermeide ich die Anwendung der adjungierten Polynome.

Ein Polynom heißt *vollreduzibel*, wenn es als Hülle von endlich oder unendlich vielen Primfunktionen darstellbar ist.

Es ist vielleicht notwendig, hier zu erwähnen, daß ein Polynom $A(y)$ endlichen Grades sehr wohl eine unendliche Anzahl von primären Teilern besitzen kann. Wenn nämlich $A(y)$ durch zwei verschiedene Polynome

$$C_1 B(y) C_1^{-1}, \quad C_2 B(y) C_2^{-1}$$

teilbar ist, so ist nach Satz 9 $A(y)$ auch durch alle $CB(y)C^{-1}$ teilbar, wo

$$C(y) = c_1 C_1(y) + c_2 C_2(y)$$

und c_1, c_2 beliebige Elemente des Konstantenkörpers sind, und hieraus erklärt sich die Möglichkeit einer unendlichen Anzahl von Teilern. Es ist auch leicht, die notwendige und hinreichende Bedingung für unendlich viele Teiler anzugeben.

Unter den Eigenschaften der vollreduziblen Polynome erwähnen wir zunächst:

Satz 1. *Ein vollreduzibles Polynom $F(y)$ hat immer eine Basisdarstellung*

$$F(y) = [P_1(y), \ldots, P_r(y)], \tag{1}$$

wo die Anzahl r der Primfunktionen der Basis gleich der Anzahl der Faktoren in einer beliebigen Primfunktionenzerlegung von $F(y)$ ist.

Wenn nämlich $P_1(y)$ ein beliebiger Primteiler von $F(y)$ ist, so ist entweder $F(y) = P_1(y)$ oder $F(y)$ ist durch eine von $P_1(y)$ verschiedene Primfunktion $P_2(y)$ teilbar; im letzten Fall ist $F(y)$ auch durch $[P_1(y), P_2(y)]$ teilbar. Dann ist entweder $F(y) = [P_1(y), P_2(y)]$ und der Satz ist bewiesen, oder es ist $F(y)$ durch eine zu $[P_1(y), P_2(y)]$ relativ prime Primfunktion $P_3(y)$, also $F(y)$ durch $[P_1(y), P_2(y), P_3(y)]$ teilbar, usw. Da der Grad von $F(y)$ endlich ist, bricht dieser Prozeß nach einer endlichen Anzahl von Schritten ab, und der Satz ist bewiesen.

Es ist nach Satz 9, Kap. I, selbstverständlich, daß, wenn $F(y)$ vollreduzibel ist, jedes mit $F(y)$ gleichartige Polynom $QF(y)Q^{-1}$ dieselbe Eigenschaft hat und

$$QF(y)Q^{-1} = [QP_1(y)Q^{-1}, \ldots, QP_r(y)Q^{-1}] \qquad \text{ist.}$$

Wir bemerken weiter, daß, wenn man ein vollreduzibles Polynom (1) als Produkt von Primfaktoren schreibt, etwa

$$F(y) = Q_r(y) \times \cdots \times Q_1(y),$$

die $P_i(y)$ in einer passenden Anordnung mit den $Q_i(y)$ paarweise gleichartig sind. Für $r = 1$ ist der Satz trivial, und der allgemeine Fall folgt leicht durch Induktion. Aus (1) erhält man nämlich

$$F(y) = [P_1 P_r(y) P_1^{-1}, \ldots, P_1 P_2(y) P_1^{-1}] \times P_1(y),$$

und da der erste Faktor rechts, wie man sofort sieht, wieder vollreduzibel mit $r - 1$ Basiselementen $P_1 P_i(y) P_1^{-1} (i = 2, \ldots, r)$ ist, so hat er eine Zerlegung in Primfaktoren, die paarweise mit den $P_i(y)$ $(i = 2, \ldots, r)$ gleichartig sind. Nach dem Hauptsatz über die Zerlegung in Primfaktoren folgt daraus das gewünschte Resultat.

[4]) Man vgl. die in der Einleitung zitierten Abhandlungen.

Satz 2. *Jeder Teiler $T(y)$ eines vollreduziblen Polynoms $F(y)$ ist wieder vollreduzibel, und die Basis von $T(y)$ kann zu einer Basis von $F(y)$ ergänzt werden.*

Nach der Konstruktionsmethode für die Basis ist klar, daß die Basis eines vollreduziblen Teilers zu einer Basis des ganzen Polynoms ergänzt werden kann. Den ersten Teil beweisen wir durch Induktion nach der Anzahl der Basiselemente von $F(y)$. Es sei $D(y)$ die Hülle von allen Primfunktionen die $T(y)$ rechts teilen; $D(y)$ ist vollreduzibel, und wir haben

$$T(y) = K(y) \times D(y), \quad F(y) = [D(y),\ P_s(y), \ldots, P_r(y)].$$

Dann ist natürlich $K(y)$ ein Teiler von

$$F(y) \times D(y)^{-1} = [DP_s(y)\,D^{-1}, \ldots, DP_r(y)\,D^{-1}],$$

folglich nach Annahme vollreduzibel, und von der Form $K(y) = DK_1(y)\,D^{\nu-1}$, wo $K_1(y)$ auch vollreduzibel ist. Daraus ergibt sich

$$T(y) = K(y) \times D(y) = [K_1(y),\ D(y)],$$

woraus man den Satz erhält.

Es ist weiter klar, daß auch jeder linke Teiler von $F(y)$ vollreduzibel ist, und daraus ergibt sich in Verbindung mit Satz 2 noch allgemeiner, daß jeder Faktor $C(y)$ von $F(y)$, der in irgendeiner Darstellung $F(y) = A(y) \times C(y) \times B(y)$ vorkommt, wieder vollreduzibel sein muß.

Die vollreduziblen Polynome können auch in der folgenden Weise charakterisiert werden:

Satz 3. *Ein Polynom $F(y)$ ist dann und nur dann vollreduzibel, wenn zwei aufeinander folgende Faktoren einer beliebigen Produktdarstellung von $F(y)$ immer umstellbar sind.*

Wir zeigen zuerst, daß $F(y)$ vollreduzibel ist, wenn alle Faktoren umstellbar sind. Wenn die Primfaktorzerlegung von $F(y)$ nur eine Primfunktion enthält, ist der Satz trivial; wir nehmen daher an, er sei für alle Polynome bewiesen, deren Primfunktionzerlegung höchstens $n-1$ Faktoren enthält, und beweisen ihn für Polynome mit n Primfaktoren. Es sei $F(y) = P_1(y) \times F_1(y)$, wo $P_1(y)$ eine Primfunktion und $F_1(y)$ nach Voraussetzung vollreduzibel ist. Dann ist aber $P_1(y) = F_1 P(y) F_1^{-1}$, und man erhält $F(y) = [P(y),\ F_1(y)]$, was mit der Behauptung äquivalent ist.

Wenn aber umgekehrt $F(y)$ vollreduzibel und $F(y) = \cdots \times A(y) \times B(y) \times \cdots$ eine beliebige Faktorzerlegung ist, so wollen wir zeigen, daß $A(y)$ mit $B(y)$ umstellbar sein muß. Nach einer früheren Bemerkung ist sowohl $B(y)$ als auch $A(y) \times B(y)$ vollreduzibel, und man kann nach Satz 2

$$A(y) \times B(y) = [B(y),\ P_1(y), \ldots, P_r(y)]$$

schreiben, wo die Primfunktionen $P_i(y)$ in $B(y)$ nicht aufgehen; daraus folgt aber

$$A(y) = B[P_1(y), \ldots, P_r(y)]\,B^{-1}.$$

Wir wollen ein vollreduzibles Polynom *gleichförmig* nennen, wenn es die Hülle von Primfunktionen derselben Art ist. In der Basisdarstellung eines gleichförmigen vollreduziblen Polynoms können natürlich nur Primfunktionen derselben Art vorkommen, und es hat daher die Form

$$F(y) = [A_1 P(y) A_1^{-1}, \ldots, A_r P(y) A_r^{-1}], \tag{2}$$

wo $P(y)$ eine Primfunktion ist. Umgekehrt ist aber jedes vollreduzible Polynom von der Form (2) gleichförmig, denn wenn $P_1(y)$ ein Primteiler von $F(y)$ ist, so muß $P_1(y)$ mit einem Faktor der Primfunktionenzerlegung von $F(y)$ gleichartig sein.

Man kann nun beweisen:

Satz 4. *Wenn $AP(y)A^{-1}$ ein beliebiger Primteiler eines gleichförmigen vollreduziblen Polynoms (2) ist, so ist $A(y)$ von der Form*

$$A(y) \equiv A_1(y) \times I_1(y) + \cdots + A_r(y) \times I_r(y) \pmod{P(y)}, \tag{3}$$

wo $I_1(y), \ldots, I_r(y)$ Eigenwurzeln von $P(y)$ sind.

Der Satz kann durch Induktion bewiesen werden; für $r = 1$ ist er nach Satz 19, Kap. I, richtig. Wir setzen $A_1 P(y) A_1^{-1} = \bar{P}(y)$; wenn $AP(y)A^{-1} = \bar{P}(y)$, so ist der Satz nach dem eben erwähnten Satz schon richtig. Im entgegengesetzten Fall ist aber das gleichförmige Polynom

$$[(\bar{P}A_2)\,P(y)\,(\bar{P}A_2)^{-1}, \ldots, (\bar{P}A_r)\,P(y)\,(\bar{P}A_r)^{-1}]$$

durch $(\bar{P}A)\,P(y)\,(\bar{P}A)^{-1}$ teilbar, und es ist nach Voraussetzung

$$\bar{P}(y) \times A(y) \equiv \bar{P}(y) \times A_2(y) \times I_2(y) + \cdots + \bar{P}(y) \times A_r(y) \times I_r(y) \pmod{P(y)}$$

oder

$$(4) \quad \bar{P}(y) \times (A(y) - A_2(y) \times I_2(y) - \cdots - A_r(y) \times I_r(y)) \equiv 0 \pmod{P(y)}.$$

Wenn nun

$$K(y) = A(y) - A_2(y) \times I_2(y) - \cdots A_r(y) \times I_r(y) \equiv 0 \pmod{P(y)},$$

so ist der Satz auch bewiesen. Wenn dies nicht der Fall ist, so schließt man aus (4)

$$A_1 P(y) A_1^{-1} = K P(y) K^{-1},$$

und folglich nach Satz 19

$$K(y) \equiv A_1(y) \times I_1(y) \pmod{P(y)},$$

woraus man die Darstellung (3) erhält.

Umgekehrt ist natürlich jede Primfunktion $AP(y)A^{-1}$, wo $A(y)$ von der Form (3) ist, wieder ein Teiler von $F(y)$, so daß man eine vollständige Übersicht über die Primteiler eines gleichförmigen, vollreduziblen Polynoms hat.

Die Hülle von allen Primfunktionen derselben Art, die ein gegebenes vollreduzibles Polynom (1) teilen, soll ein größter gleichförmiger Teiler von $F(y)$ heißen. Man zeigt dann ohne Schwierigkeit:

Satz 5. *Jedes vollreduzible Polynom kann eindeutig als Hülle von größten gleichförmigen Teilern dargestellt werden.*

Genau so wie wir hier rechtsseitig vollreduzible Polynome eingeführt haben, kann man auch linksseitig vollreduzible Polynome definieren. Ein Polynom $F(y)$ heißt also *links vollreduzibel*, wenn es eine linksseitige Hülle von Primfunktionen ist. Die Existenz einer Basis für $F(y)$ folgt wie früher, und der Satz 2 gilt unverändert für linke Teiler. Aus Satz 3 schließt man aber sofort:

Satz 6. *Jedes links vollreduzible Polynom ist auch rechts vollreduzibel und umgekehrt.*

Nach den früheren Bemerkungen ist auch klar, daß bei linken und rechten Basisdarstellungen desselben vollreduziblen Polynoms immer dieselbe Anzahl von Basiselementen vorkommen muß und die Basiselemente paarweise von derselben Art sein müssen.

2. Darstellungen als Produkt von vollreduziblen Faktoren.

Wir wollen nun diese Resultate zu einigen Untersuchungen über Normaldarstellungen von Differentialpolynomen benutzen. Wir beweisen zuerst einen wichtigen Satz von Loewy [5]).

Es sei $F(y)$ ein beliebiges Polynom; die Hülle $H_1(y)$ aller Primfunktionen $P(y)$, welche $F(y)$ rechts teilen, ist dann, wie man leicht sieht, der vollreduzible Faktor höchsten Grades, der $F(y)$ teilt. Es soll daher $H_1(y)$ der *größte rechtsseitige vollreduzible Teiler* von $F(y)$ heißen. $H_1(y)$ ist eindeutig bestimmt, und jeder andere vollreduzible Teiler von $F(y)$ ist ein Teiler von $H_1(y)$. Wir schreiben $F(y) = F_1(y) \times H_1(y)$, und $F_1(y)$ hat wieder einen eindeutigen größten vollreduziblen Teiler $H_2(y)$ usw. Wir erhalten daher den Satz:

Satz 7. (Loewy.) *Jedes Differentialpolynom hat eine eindeutige Zerlegung in rechtsseitige größte vollreduzible Faktoren:*

$$(5) \qquad F(y) = a_0 H_h(y) \times \cdots \times H_2(y) \times H_1(y).$$

[5]) Math. Ann. **62** (1906), S. 89—117.

Wir wollen weiter den folgenden Satz beweisen, der für verschiedene Anwendungen nützlich ist:

Satz 8. *Es sei $F_1(y)$ ein Teiler von $F(y)$ und*

$$F_1(y) = b_0 G_k(y) \times \cdots \times G_2(y) \times G_1(y) \tag{6}$$

eine Zerlegung von $F(y)$ in (nicht notwendige größte) vollreduzible Faktoren. Wenn dann $F(y)$ die Zerlegung (5) in größte vollreduzible Faktoren besitzt, so ist jedes Produkt $G_i(y) \times \cdots \times G_1(y)$ $(i = 1, 2, \ldots, h)$ ein Teiler von $H_i(y) \times \cdots \times H_1(y)$.

Nach der Definition des größten vollreduziblen Faktors $H_1(y)$ muß $G_1(y)$ ein Teiler von $H_1(y)$ sein; der allgemeine Satz kann daher durch Induktion bewiesen werden, und wir nehmen an, es sei schon gezeigt, daß

$$H_{i-1}(y) \times \cdots \times H_1(y) = K_{i-1}(y) \times G_{i-1}(y) \times \cdots \times G_1(y). \tag{7}$$

Aus der Gleichung $F(y) = L(y) \times F_1(y)$ erhält man dann leicht nach (5), (6) und (7)

$$a_0 H_h(y) \times \cdots \times H_i(y) \times K_{i-1}(y) = L(y) \times b_0 y \times G_k(y) \times \cdots \times G_i(y);$$

nach Satz 5, Kap. I, ist aber das Produkt $H_h(y) \times \cdots \times H_i(y)$ durch das vollreduzible Polynom $K_{i-1} G_i(y) K_{i-1}^{-1}$ teilbar, und da $H_i(y)$ der größte vollreduzible Faktor des Produkts ist, so muß man

$$H_i(y) = T(y) \times K_{i-1} G_i(y) K_{i-1}^{-1}$$

haben. Nach Multiplikation mit $K_{i-1}(y)$ erhält man

$$H_i(y) \times K_{i-1}(y) = T(y) \times [K_{i-1}(y), G_i(y)] = K_i(y) \times G_i(y),$$

und wenn man hier rechts mit $G_{i-1}(y) \times \cdots \times G_1(y)$ multipliziert und mit (7) vergleicht, so erhält man die gewünschte Identität

$$H_i(y) \times \cdots \times H_1(y) = K_i(y) \times G_i(y) \times \cdots \times G_1(y).$$

Wir wenden nun den Satz 8 auf den Fall an, wo der Teiler $F_1(y)$ mit $F(y)$ identisch ist. Es folgt dann aus (7) für $i = k$, indem wir $k \geqq h$ annehmen,

$$H_k(y) \times \cdots \times H_1(y) = K_k(y) \times G_k(y) \times \cdots \times G_1(y) = K_k(y) \times F(y),$$

und es wird somit $F(y)$ ein echter Teiler von sich selbst. Dieser Widerspruch gibt uns den folgenden Satz:

Satz 9. *Eine Zerlegung eines Polynoms in beliebige vollreduzible Faktoren enthält nie weniger Faktoren als die Zerlegung in größte vollreduzible Faktoren.*

Genau dieselben Sätze gelten auch für die Zerlegung eines Polynoms in linksseitige vollreduzible Faktoren.

Wir wollen nun der Einfachheit wegen $F(y)$ primär annehmen. Die eindeutige Zerlegung von $F(y)$ in linksseitige größte vollreduzible Faktoren ist nach Satz 6 auch eine Zerlegung in rechtsseitige vollreduzible Faktoren, und es folgt nach Satz 9, daß die linksseitige Zerlegung mindestens so viele Faktoren besitzen muß als die Zerlegung in rechtsseitige größte vollreduzible Faktoren, und durch die entsprechenden Schlüsse zeigt man auch das umgekehrte. Verbindet man dies mit Satz 8, so erhält man:

Satz 10. (Loewy)[6]. *Die Zerlegungen*

$$F(y) = H_h(y) \times \cdots \times H_1(y) = L_h(y) \times \cdots \times L_1(y)$$

eines primären Polynoms $F(y)$ in rechte bzw. linke größte vollreduzible Faktoren haben immer dieselbe Anzahl von Faktoren, und es ist

$$H_i(y) \times \cdots \times H_1(y) \equiv 0 \pmod{L_i(y) \times \cdots \times L_1(y)}$$

und

$$(\text{mod } H_h(y) \times \cdots \times H_i(y))\, L_h(y) \times \cdots \times L_i(y) \equiv 0 \quad (i = 1, 2, \ldots, h).$$

[6]) Sitzungsberichte der Heidelberger Akad. Jahrg. 1917, 8. Abh. Man vgl. auch die analogen Untersuchungen von Krull: „Theorie und Anwendung der verallgemeinerten Abelschen Gruppen". Sitzungsber. der Heidelberger Akad. Jahrg. 1926, 1. Abh.

3. Darstellung eines Polynoms als Hülle von unzerlegbaren Polynomen.

Ein Polynom $F(y)$ soll *zerlegbar* heißen, wenn es in der Form

$$F(y) = [A(y), B(y)] \tag{8}$$

dargestellt werden kann, wo $A(y)$ zu $B(y)$ relativ prim ist; im entgegengesetzten Fall heißt $F(y)$ *unzerlegbar*. Der folgende Hilfssatz über zerlegbare Polynome ist oft nützlich:

Satz 11. *Wenn $F(y)$ zerlegbar ist und die Zerlegung* (8) *hat, so ist jeder durch $A(y)$ teilbare Teiler $C(y)$ von $F(y)$ auch zerlegbar mit der Zerlegung*

$$C(y) = [A(y), (B(y), C(y))]. \tag{9}$$

Es ist klar, daß die rechte Seite von (9) ein Teiler von $C(y)$ ist; um das umgekehrte zu zeigen, setzen wir

$$C(y) = C_1(y) \times A(y), \qquad F(y) = F_1(y) \times C(y),$$

und aus (8) folgt dann nach Division mit $A(y)$

$$AB(y)\,A^{-1} = F_1(y) \times C_1(y).$$

Nach Satz 8, Kap. I, ist daher $C_1(y) = AD(y)\,A^{-1}$, also $C(y) = [A(y), D(y)]$, wo $D(y)$ ein Teiler von $B(y)$ ist.

Wenn in (8) die Polynome $A(y)$ und $B(y)$ weiter zerlegbar sind, so erhält man nach fortgesetzter Zerlegung:

Satz 12. *Jedes Polynom $F(y)$ hat eine Zerlegung als Hülle von unzerlegbaren totalprimen Polynomen*

$$F(y) = [K_1(y), \ldots, K_r(y)] \tag{10}$$

Dabei heißen natürlich r Polynome $K_i(y)$ $(i = 1, 2, \ldots, r)$ totalprim, wenn ein beliebiges $K_i(y)$ zu der Hülle der übrigen relativ prim ist. Für totalprime Polynome hat man

Satz 13. *Wenn die Polynome $K_i(y)$ $(i = 1, 2, \ldots, r)$ totalprim sind, so haben die Kongruenzen*

$$X(y) \equiv A_i(y) \pmod{K_i(y)} \qquad (i = 1, 2, \ldots, r) \tag{11}$$

eine eindeutige Lösung mod $[K_1(y), \ldots, K_r(y)]$, *für beliebige Polynome $A_i(y)$ $(i = 1, 2, \ldots, r)$.*

Die Eindeutigkeit mod $[K_1(y), \ldots, K_r(y)]$ folgt sofort. Setzt man

$$\bar{K}_i(y) = [K_1(y), \ldots, K_{i+1}(y),\ K_{i-1}(y), \ldots, K_r(y)],$$

so kann man ein $R_i(y)$ so bestimmen, daß

$$R_i(y) \times \bar{K}_i(y) \equiv A_i(y) \pmod{K_i(y)},$$

und

$$X(y) \equiv \sum_{i=1}^{r} R_i(y) \times \bar{K}_i(y) \pmod{[K_1(y), \ldots, K_r(y)]}$$

ist die gewünschte Lösung.

Es entsteht nun natürlich die Frage nach der Eindeutigkeit der Zerlegung (10). Unter Anwendung seiner Theorie der verallgemeinerten Abelschen Gruppen hat **Krull**[7]) bewiesen, daß die unzerlegbaren Faktoren in zwei Darstellungen paarweise von derselben Art sein müssen. Wir wollen etwas schärfer beweisen:

Satz 14. *Zwei verschiedene Darstellungen eines Polynoms als Hülle von totalprimen unzerlegbaren Faktoren haben immer dieselbe Anzahl von Faktoren, und die Faktoren müssen paarweise von derselben Art sein. Weiter kann ein unzerlegbarer Faktor $K(y)$ der einen Zerlegung immer einen Faktor $L(y)$ der zweiten Zerlegung ersetzen, und jedes $L(y)$ ist durch ein $K(y)$ ersetzbar.*

Der folgende Beweis scheint mir wesentlich einfacher als der Beweis von Krull; es ist auch von Interesse zu bemerken, daß man durch dieselbe Methode auch einen

[7]) Math. Zeitschrift **23** (1925), S. 161—196.

einfachen Beweis des Wedderburnschen Satzes über die Darstellung einer Gruppe als direktes Produkt von direkt unzerlegbaren Faktoren erhält.

Der Beweis folgt durch Induktion, indem man annimmt, daß der Satz für alle Polynome niedrigeren Grades als $F(y)$ richtig sei. Wenn nun

$$F(y) = [L_1(y), \ldots, L_s(y)] \tag{12}$$

eine zweite Zerlegung von $F(y)$ ist, so wollen wir zuerst zeigen:

Es gibt ein $L_i(y)$ oder ein $K_i(y)$, das ein $K_j(y)$ bzw. ein $L_j(y)$ in den Darstellungen (10) *und* (12) *ersetzen kann.*

Wir nehmen $r \leqq s$ an; weiter sei $P(y)$ ein beliebiger Primteiler eines der $K_i(y)$; wir wollen $K_r(y) = \bar{K}_r(y) \times P(y)$ annehmen. Es ist dann bequem, zwei Fälle zu unterscheiden:

Fall I. $P(y)$ ist ein Teiler einer Hülle von weniger als s der Faktoren $L_i(y)$. Wir können die Bezeichnung so wählen, daß

$$L(y) = [L_2(y), \ldots, L_s(y)] = \bar{L}(y) \times P(y),$$

und es folgt aus (10) und (12), wenn man mit $P(y)$ dividiert,

$$[PK_1(y)P^{-1}, \ldots, PK_{r-1}(y)P^{-1}, \bar{K}_r(y)] = [PL_1(y)P^{-1}, \bar{L}(y)], \tag{13}$$

und durch Gradvergleichung sieht man, daß beide Seiten nur totalprime Faktoren enthalten. Nach Voraussetzung gilt der Satz für das Polynom (13), und es muß daher das unzerlegbare Polynom $PL_1(y)P^{-1}$ einen unzerlegbaren Faktor der linken Seite ersetzen können. Wir unterscheiden zwei Unterfälle:

a) $PL_1(y)P^{-1}$ ersetzt ein $PK_i(y)P^{-1}$, z. B. $PK_1(y)P^{-1}$. Man erhält dann aus (13) nach Multiplikation mit $P(y)$

$$F(y) = [L_1(y), K_2(y), \ldots, K_r(y)].$$

b) $PL_1(y)P^{-1}$ ersetzt einen unzerlegbaren Faktor von $\bar{K}_r(y)$. Man erhält dann in derselben Weise aus (13) eine Darstellung

$$F(y) = [K_1(y), \ldots, K_{r-1}(y), \; L_1(y), \; \bar{\bar{K}}_r(y) \times P(y)]. \tag{14}$$

Dies ist aber unmöglich, denn wenn man (10) und (14) durch

$$K(y) = [K_1(y), \ldots, K_{r-1}(y)]$$

dividiert so erhält man

$$KK_r(y)K^{-1} = [KL_1(y)K^{-1}, \; K(\bar{\bar{K}}_r(y) \times P(y))K^{-1}],$$

woraus leicht folgen würde, daß $K_r(y)$ zerlegbar wäre.

Fall II. Man kann in diesem Fall voraussetzen, daß jedes $K_i(y)$ zu der Hülle von $s-1$ beliebigen $L_i(y)$ relativ prim ist. Da $r \leqq s$ war, so muß es ein $K_i(y)$ und ein $L_j(y)$ so geben, daß der Grad von $K_i(y)$ nicht kleiner als der Grad von $L_j(y)$ ist. Dann ist aber

$$F(y) = [L_1(y), \ldots, K_i(y), \ldots, L_s(y)],$$

denn die rechte Seite ist jedenfalls ein Teiler von $F(y)$ und der Grad kann nach den Voraussetzungen nicht kleiner als der Grad von $F(y)$ sein.

Der erste Teil des Beweises ist dadurch vollendet. Wir wählen nun die Bezeichnung so, daß

$$F(y) = [L_1(y), \; K_2(y), \ldots, K_r(y)]. \tag{15}$$

Aus (15) folgt zunächst, daß $r = s$ ist und daß die $K_i(y)$ paarweise mit den $L_i(y)$ von derselben Art sind.

Dividiert man nämlich (10) und (15) durch $K(y)$, so erhält man

$$KK_1(y)K^{-1} = KL_1(y)K^{-1}$$

und weiter aus (12) und (15)

$$[L_1L_2(y)L_1^{-1}, \ldots, L_1L_s(y)L_1^{-1}] = [L_1K_2(y), \ldots, L_1K_r(y)L_1^{-1}]. \tag{16}$$

Nach Voraussetzung müssen hier beide Seiten dieselbe Anzahl von unzerlegbaren Faktoren enthalten, und die unzerlegbaren Polynome $L_1 L_i(y) L_1^{-1}$ und $L_1 K_i(y) L_1^{-1}$ müssen paarweise von derselben Art sein.

Es bleibt daher nur übrig, aus (15) die Ersetzbarkeit aller $L_i(y)$ und $K_i(y)$ abzuleiten.

In (16) kann man nach Voraussetzung ein beliebiges $L_1 L_i(y) L_1^{-1}$ durch ein $L_1 K_i(y) L_1^{-1}$ ersetzen, und wenn man dies ausführt und nachher mit $L_1(y)$ multipliziert, so erhält man

$$F(y) = [L_1(y), \ldots, K_i(y), \ldots, L_r(y)]. \tag{17}$$

Jedes $L_i(y)$ $(i \geqq 2)$ kann also durch ein $K_i(y)$ $(i \geqq 2)$ ersetzt werden, und jedes solche $K_i(y)$ kann zu einem solchen Ersatz benutzt werden.

Aus (17) folgt aber umgekehrt in derselben Weise, daß jedes $K(y)$ durch ein $L(y)$ ersetzt werden kann, und daß jedes $L(y)$ zu einem Ersatz benutzt werden kann. Die einzige Ausnahme bildet das Paar $K_i(y)$, $L_i(y)$, aber wenn $r \geqq 3$ ist, kann man eine zweite Darstellung (17) betrachten, worin $K_j(y)$ an der Stelle $K_i(y)$ auftritt. Wenn $r \geqq 3$, ist daher die gewünschte Eigenschaft für alle $L(y)$ bewiesen. Aus einer beliebigen Darstellung

$$F(y) = [K_1(y), \ldots, L_i(y), \ldots, K_r(y)]$$

folgt aber auch, daß $K_1(y)$ durch ein $L(y)$ und $L_1(y)$ durch ein $K(y)$ ersetzt werden kann, womit der Satz bewiesen ist.

Der Ausnahmefall

$$F(y) = [K_1(y), K_2(y)] = [L_1(y), K_2(y)] = [L_1(y), L_2(y)] \tag{18}$$

bleibt aber übrig. Um hier die Ersetzbarkeit von $L_1(y)$ durch ein $K(y)$ zu zeigen, muß man beweisen, daß unter den beiden Gleichungen

$$F(y) = [K_1(y), L_2(y)], \quad F(y) = [K_2(y), L_2(y)] \tag{19}$$

wenigstens eine richtig ist. Wenn aber $G(y) = [K_1(y), L_2(y)]$ nur ein Teiler von $F(y)$ ist, so hat man nach Satz 11

$$G(y) = [K_1(y), (G(y), K_2(y))] = [(G(y), L_1(y)), L_2(y)]. \tag{20}$$

Da hier $(G(y), K_2(y))$ von niedrigerem Grade als $L_2(y)$ ist, so muß in (20) $K_1(y)$ durch $L_2(y)$ ersetzbar sein. Dann erhält man aber

$$F(y) = [G(y), K_2(y)] = [L_2(y), (G(y), K_2(y)), K_2(y)] = [L_2(y), K_2(y)].$$

In derselben Weise beweist man die Ersetzbarkeit der übrigen Faktoren in (18).

Die Darstellung eines Polynoms $F(y)$ als Hülle von totalprimen unzerlegbaren Faktoren ist im allgemeinen nicht eindeutig; die verschiedenen Darstellungen sind aber eng mit den Eigenwurzeln von $F(y)$ verbunden. Wenn nämlich (10) eine Zerlegung von $F(y)$ ist, so hat nach Satz 14 eine beliebige andere Zerlegung die Form

$$F(y) = [A_1 K_1(y) A_1^{-1}, \ldots, A_r K_r(y) A_r^{-1}]. \tag{21}$$

Die Kongruenzen

$$I(y) \equiv A_i(y) \times I_i(y) \pmod{K_i(y)},$$

wo $I_i(y)$ eine zu $K_i(y)$ relativ prime Eigenwurzel von $K_i(y)$ ist, hat nach Satz 13 immer eine Lösung $I(y)$. $I(y)$ ist dann offenbar eine Eigenwurzel von $F(y)$, und umgekehrt gibt jede zu $F(y)$ relativ prime Eigenwurzel eine Darstellung (21). Es ist also bewiesen:

Satz 15. *Wenn* (10) *eine Darstellung von* $F(y)$ *als Hülle von totalprimen unzerlegbaren Polynomen ist, so hat jede andere Darstellung die Form*

$$F(y) = [IK_1(y) I^{-1}, \ldots, IK_r(y) I^{-1}],$$

wo $I(y)$ *eine zu* $F(y)$ *relativ prime Eigenwurzel von* $F(y)$ *ist.*

Eingegangen 30. Januar 1932.

Journal für die reine und angewandte Mathematik

gegründet von A. L. Crelle 1826

Herausgegeben von

K. Hensel

H. Hasse L. Schlesinger

Wissenschaftlicher Beirat

H. Brandt / M. Dehn / G. Doetsch / A. Fraenkel / O. Haupt / F. Hausdorff
E. Hellinger / G. Kowalewski / H. Rademacher / K. Reidemeister
A. Rosenthal / C. Schaefer / W. Schmeidler / F. Schottky / O. Toeplitz

Band 169

In 4 Heften

Walter de Gruyter & Co.

vormals G. J. Göschen'sche Verlagshandlung — J. Guttentag, Verlagsbuchhandlung — Georg Reimer — Karl J. Trübner — Veit & Comp.

Berlin W 10 und Leipzig

1933